IPA® Software Engineering Center
Information-technology Promotion Agency, Japan

SEC統合系プロジェクトの取組み紹介
～統合システムの安全性・信頼性の確保に向けて～

2011年６月16日

（独）情報処理推進機構
ソフトウェア・エンジニアリング・センター
統合系プロジェクトリーダー
立石 譲二

1. ソリューション技術としてのITから見た社会の抱える課題

➢ 世界・日本は気候変動、水、交通、医療・介護等の様々な社会的課題を抱えている。

世界・日本の抱える課題（例）

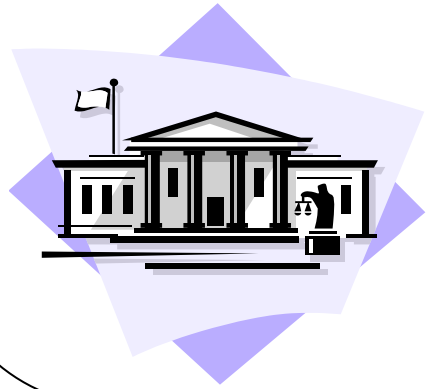
気候変動問題

水資源問題

交通問題

医療・介護問題

電子政府



物流効率化

中小企業支援

地域活性化

ITによる産業の高次化と社会システムの革新　～「スマートコミュニティ」～

経済産業省

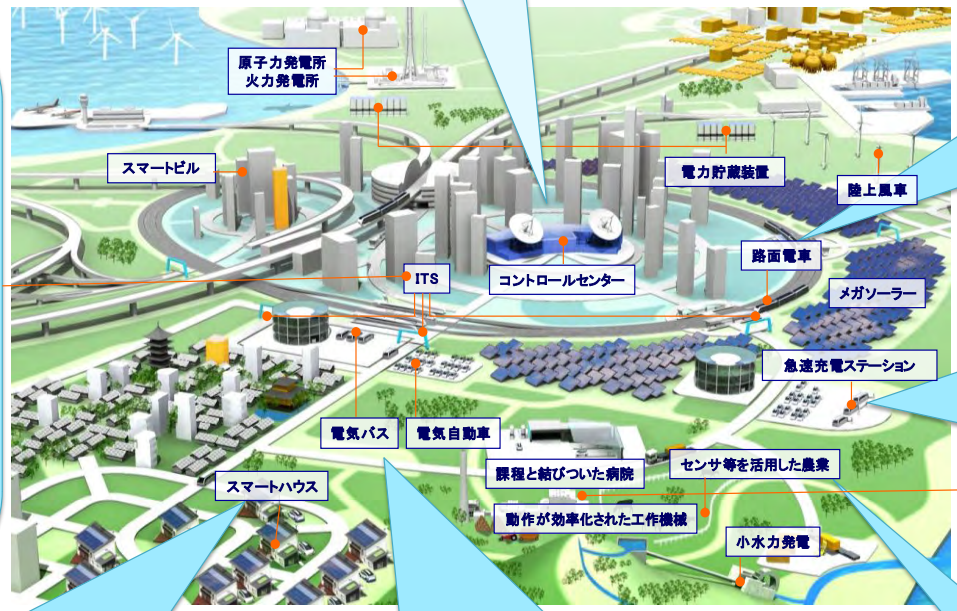
コントロールセンター

地域のエネルギー需給を最適化するコントロールセンター

- 太陽光発電、風力発電、小水力など自然エネルギーを電源として積極的に活用
- 変動の多い自然エネルギーを地域内で有効活用するため、各家庭やオフィスで余った電力を地域内で融通
- 電気バスや電気自動車の位置情報と充電状態を管理することで、これらの自動車を電力インフラとして活用

エネルギーネットワークと一体になった新しい交通インフラ

EVや電気バス同士で情報をやりとりすることにより、
飛躍的な低炭素化と事故や渋滞問題の解決を同時実現



架線レス路面電車

蓄電池を搭載した路面電車
駅での停車時：電池に充電
駅間の移動時：電池で駆動

急速充電ステーション

30分で80%充電

医療／ものづくりなど

・テーラーメード化された医療の提供
・GPSを活用した自動車両誘導システム

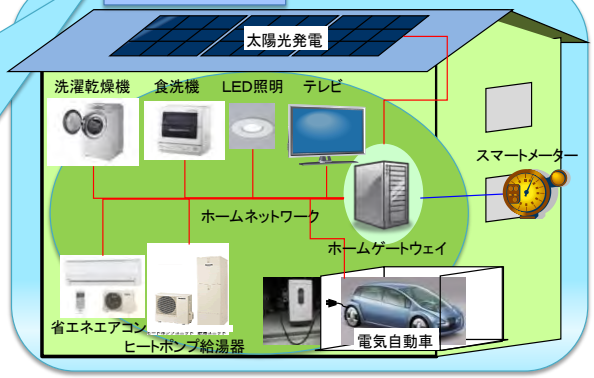
センサ等を活用した農業

各種情報を分析し、
最適な生産手段を可能に

EVを電力インフラとして活用

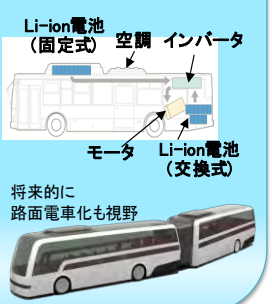
電力不足時：電気自動車→家庭
電力過剰時：家庭→電気自動車

スマートハウス



電気バス（将来は路面電車化）

電池交換式の電気バス。将来的には複数台を連結して路面電車化



（出所）スマートコミュニティ関連システムフォーラム資料、三菱重工資料より経済産業省作成

（参考1）ITを活用した交通システム分野での課題解決例

SEC Software Engineering

➢ GPS・センサ情報と運転者の情報を組み合わせることによって、個人にマッチした情報提供や縦列走行などの自律運転といった交通システムの革新が実現。

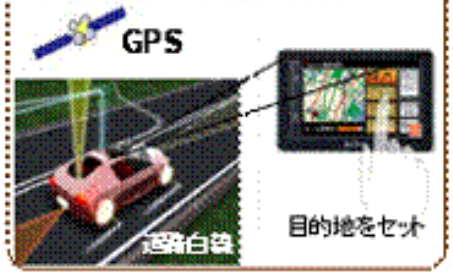
センサ・GPSからの道路・運転者情報を活用した交通システムの革新

個人向けの情報提供

運転者の情報(趣向等)とGPS情報(車体の位置情報等)を組み合わせ、一人一人にマッチした情報を最適な場所で提供可能に

省エネ運転制御技術

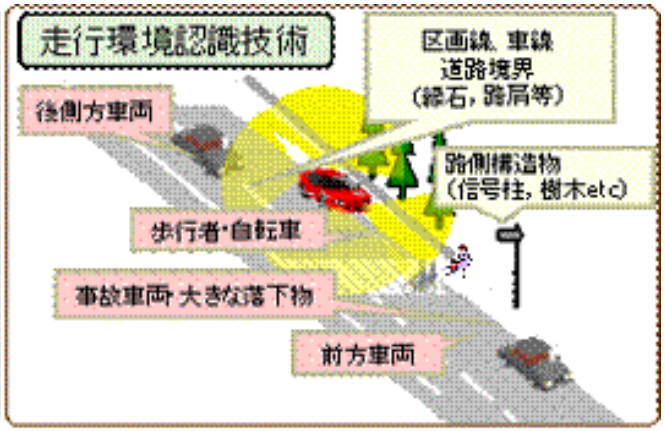
燃費のよいルート案内
エコドライブの自動化
接近隊列走行による空気抵抗低減



走行制御技術

高精度GPS＋3次元道路地図利用による自律走行制御

走行環境認識技術



位置認識技術

車車間通信技術

（出所）NEDO資料、経済産業省「クラウド・コンピューティングと日本の競争力に関する研究会」第3回資料

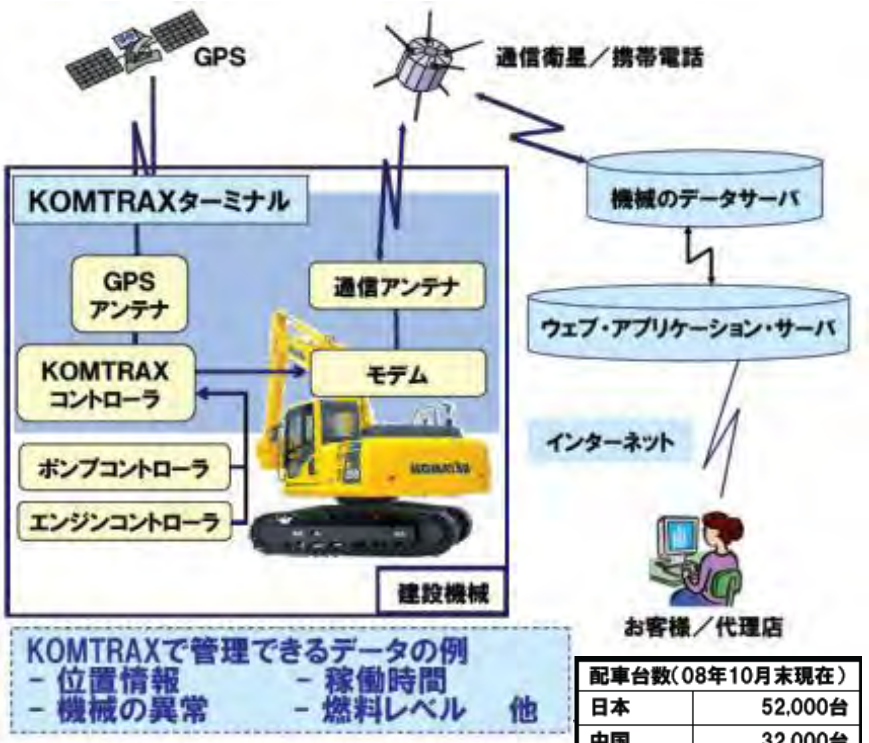
（参考2）クラウド・コンピューティングを活用したものづくり面でのイノベーション

SEC

- 製品に通信アンテナを搭載することによって、GPS・衛星を活用し、製品単位での盗難防止や異常管理、需給予測などが可能になるとともに、自動での車両誘導等が実現。

センサ・GPSからの製品情報を活用した管理システム

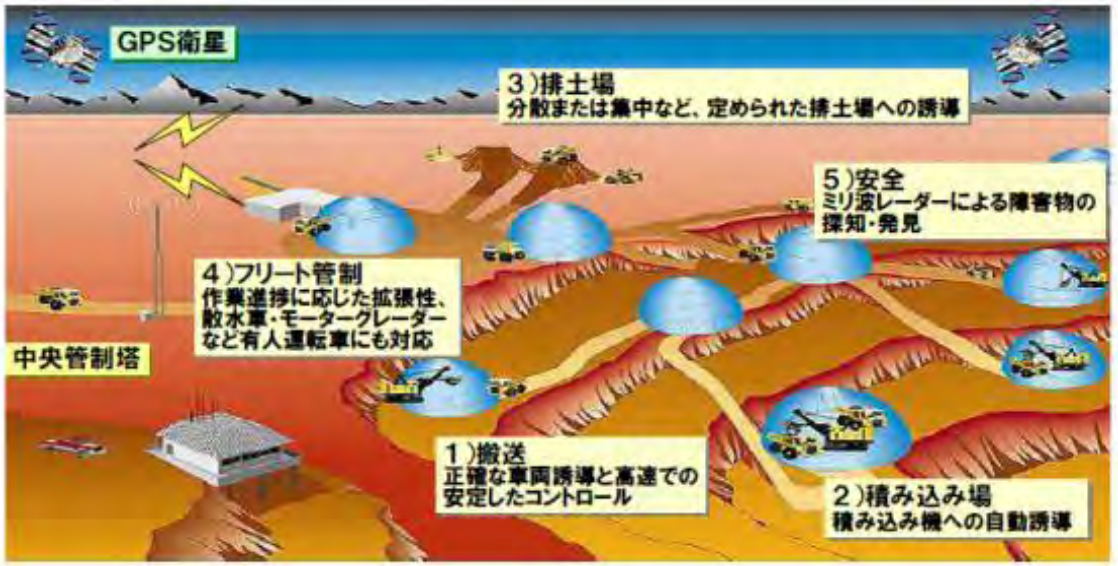
機械稼働管理システム（KOMTRAX）



KOMTRAXで管理できるデータの例
- 位置情報　- 稼働時間
- 機械の異常　- 燃料レベル　他

配車台数（08年10月末現在）	
日本	52,000台
中国	32,000台
北米	17,000台
欧州、他	19,000台
計	約120,000台

無人ダンプトラック運行システム



（注）KOMTRAX：Komatsu Machine Tracking System

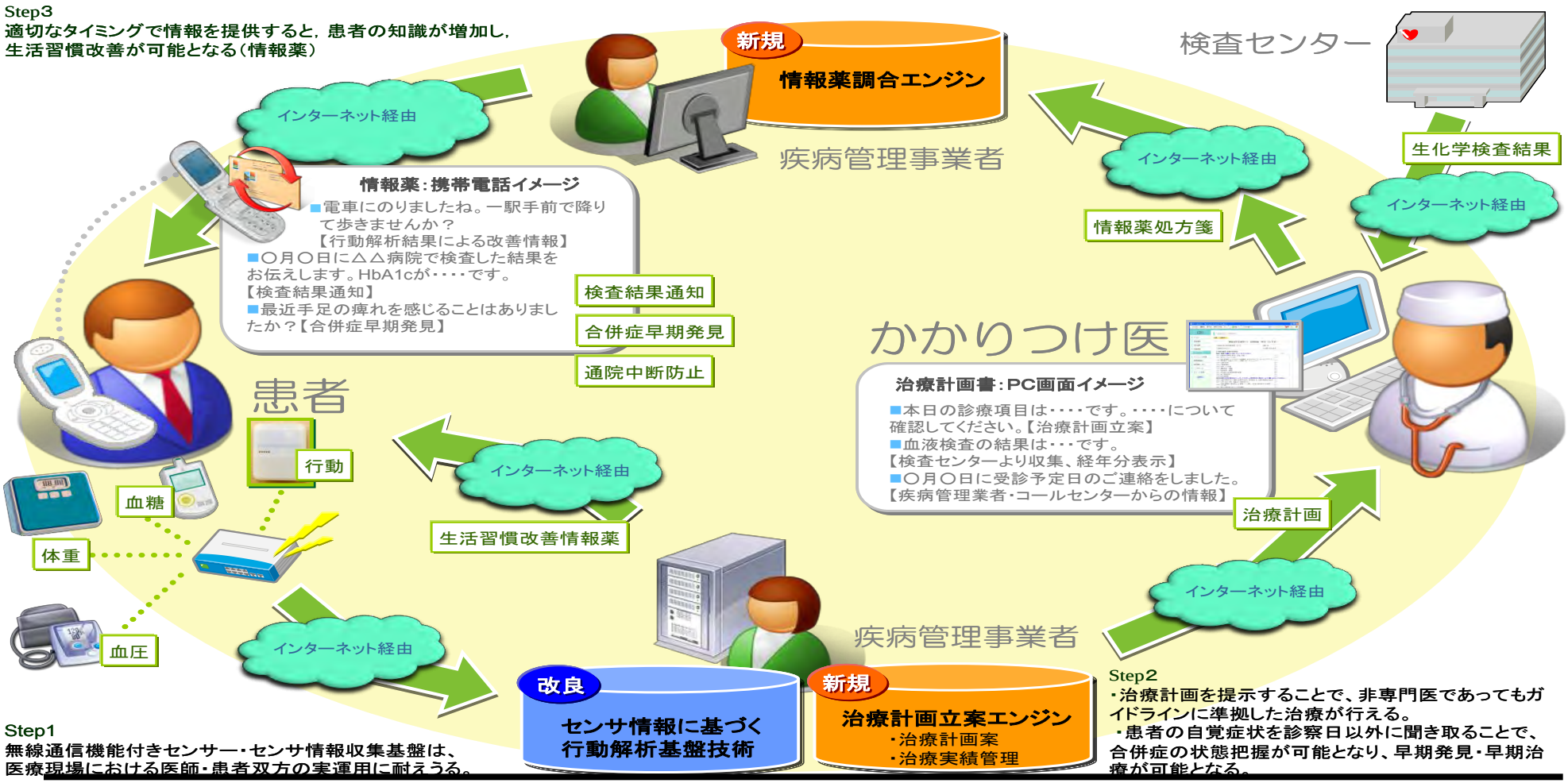
（出所）コマツ

（参考3）ITを活用したヘルスケア分野での課題解決例

SEC

➢ 患者の行動や健康情報を携帯のGPSや健康器具のセンサによって収集し、ネット上で医師や患者自身、疾病管理事業者と共有することで、患者一人一人にテーラーメイドされた治療や生活改善のための情報を「情報薬」として処方するサービスが実現。

センサ・GPSからの健康情報を活用した健康管理システム



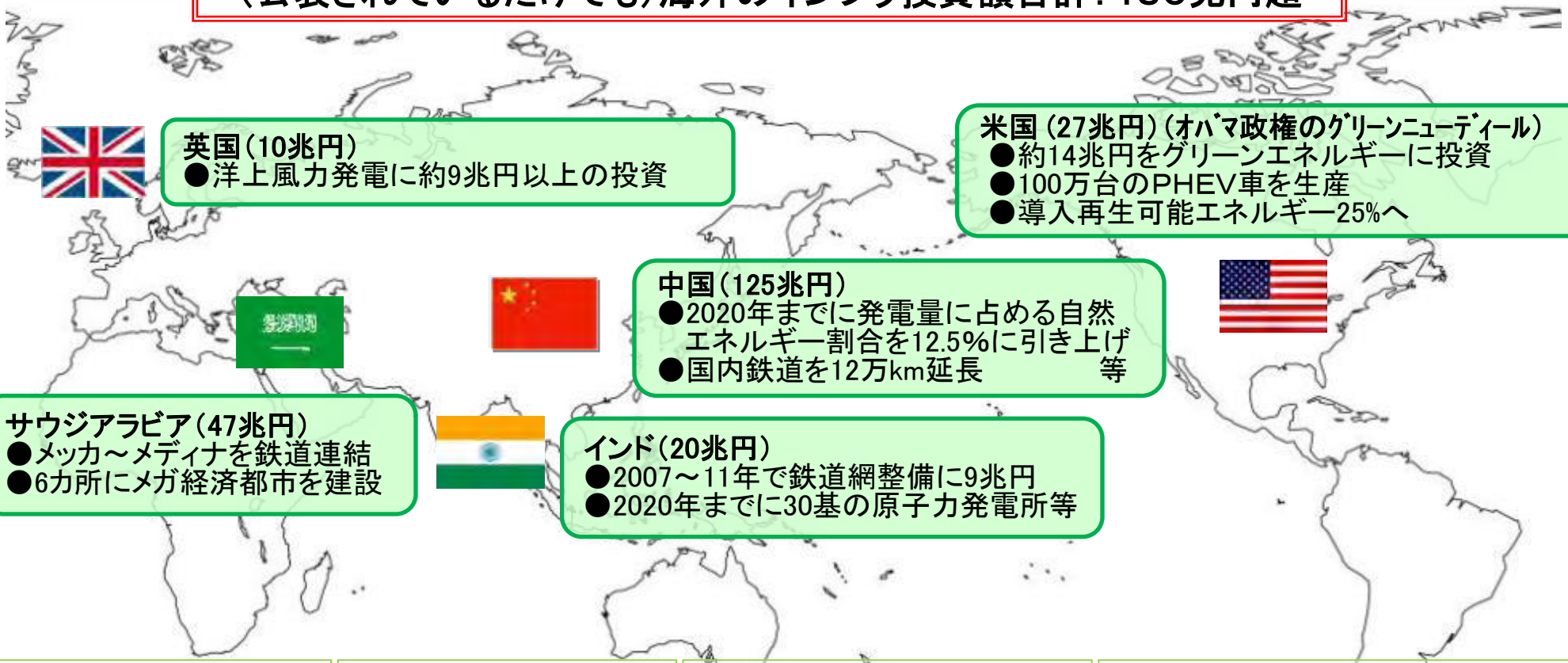
（出所）経済産業省「クラウド・コンピューティングと日本の競争力に関する研究会」第3回資料

（参考4）グリーン分野を中心とした海外の膨大なインフラ投資

SEC

➢ 先進国・新興国を問わず、グリーン分野を中心に巨額のインフラ投資を次々と計画。

（公表されているだけでも）海外のインフラ投資額合計：430兆円超



英国（10兆円）
●洋上風力発電に約9兆円以上の投資

米国（27兆円）（ｵﾊﾞﾏ政権のｸﾞﾘｰﾝﾆｭｰﾃﾞｨｰﾙ）
●約14兆円をグリーンエネルギーに投資
●100万台のPHEV車を生産
●導入再生可能エネルギー25%へ

中国（125兆円）
●2020年までに発電量に占める自然エネルギー割合を12.5%に引き上げ
●国内鉄道を12万km延長　等

サウジアラビア（47兆円）
●メッカ～メディナを鉄道連結
●6カ所にメガ経済都市を建設

インド（20兆円）
●2007～11年で鉄道網整備に9兆円
●2020年までに30基の原子力発電所等

コンゴ（7.4兆円）
●コンゴ川に世界最大の水力発電ダムを建設

ロシア（69兆円）
●2030年までにシベリア鉄道を近代化

メキシコ（29.7兆円）
●5カ年の国家インフラ計画
●輸送・通信分野で巨額投資

ブラジル（32兆円）
●リオデジャネイロ～サンパウロに高速鉄道

その他：台湾（11兆円）、南アフリカ共和国（9兆円）、タイ（5.9兆円）、ベトナム（5.8兆円）、イラク（4.5兆円）、韓国（4兆円）、フランス（3.4兆円）など

（参考5）世界最高水準のサービス品質を誇る日本の社会インフラ

SEC

- 日本の社会インフラは、世界最高水準のサービス品質。
- サービス品質には、ITの高度制御が大きく貢献。（インフラ投資全体の中で一定程度の割合を占める。）

（例）我が国の電力、鉄道、水道のおけるサービス品質の比較優位性

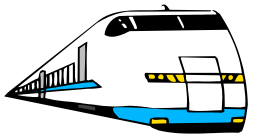
電力 ： 年間平均停電時間

日本 4分 ＞ ドイツ 37分 ＞ 米国 97分 ＞ 中国 800分

水道 ： 漏水率

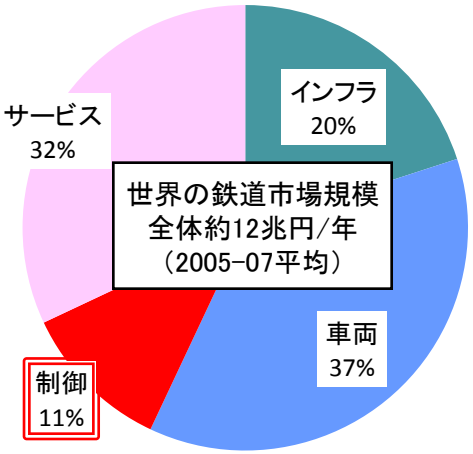
日本（東京） 3．6% ＞ 米国（ﾛｻﾝｾﾞﾙｽ） 9% ＞ イギリス（ﾛﾝﾄﾞﾝ） 26．5% ＞ タイ（ﾊﾞﾝｺｸ） 33%

鉄道 ： 定時発着率比較



日本 99% ＞ イギリス 88% ＞ タイ 63% ＞ マレーシア 43%

（例）鉄道インフラに占めるITの高度制御 ： 世界で毎年1.3兆円の投資



（鉄道制御システム）

ITの高度制御によって、車両、運行管理・信号システム、変電システム、旅客サービス等を統合。

（出所）東芝HP、日立製作所HP、MURC「IT産業の社会インフラ分野への国際展開調査（JIPDEC委託）」、経済産業省「水ビジネス国際展開研究会」

2. 統合システムの信頼性について
国民生活に直結する情報システムの信頼性（国内編）

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

日付	不具合事例	不具合原因
2007年3月2日	au3機種64万台に不具合 使い方によってフル充電できず、電池劣化が進行する可能性	充電機能のソフトウェア不具合
2007年5月27日	全日空国内線予約システム故障 130便が欠航、影響は4万人以上、キャンセルなどによる損失4.5億円	空港端末とホストコンピュータをつなぐルータ管理プログラムの設定ミスによるメモリー故障が発端で全システムに波及
2007年10月12日 2007年10月18日	自動改札機起動せず PASMO-Suica窓口処理機で異常発生	ともに、中央コンピュータからのデータをICカードに書き込むプログラムにミス
2008年7月22日	東京証券取引所のシステム障害 東証株価指数やTOPIXオプション、国債先物取引などの派生商品の売買不可	単純なプログラムミス（4けたの数字を入力しなければならないところを誤って「4」と入力）
2009年8月28日	北米トヨタ車レクサスの暴走による死亡事故 レクサスが高速道路で暴走し、ブレーキが効かず運転手含む4名が死亡。フロアマットの改修と230万台のリコールを実施。	フロアマットとは別に、スロットル電子制御システムの欠陥の疑いが議会から追求されNASAでの検証が行われたが、プログラム上の不具合は発見されず。開発者側のシステム品質の説明力の限界を印象づけた出来事
2011年3月18日	みずほ銀行 3月15日から特定口座の振り込み処理で発生したシステムトラブルを発端に全てのATMの利用及び振り込み処理が停止し、給与振り込み等最大116万件の決済処理が滞った。	被災地義援金を募集した都内一部支店の複数口座について、システム上の上限を超える取引が集中した結果、約一週間に及ぶ大規模なシステム障害に発展した。義援金受付口座に対する行員の上限設定ミス

国民生活に直結する情報システムの信頼性（全世界編）

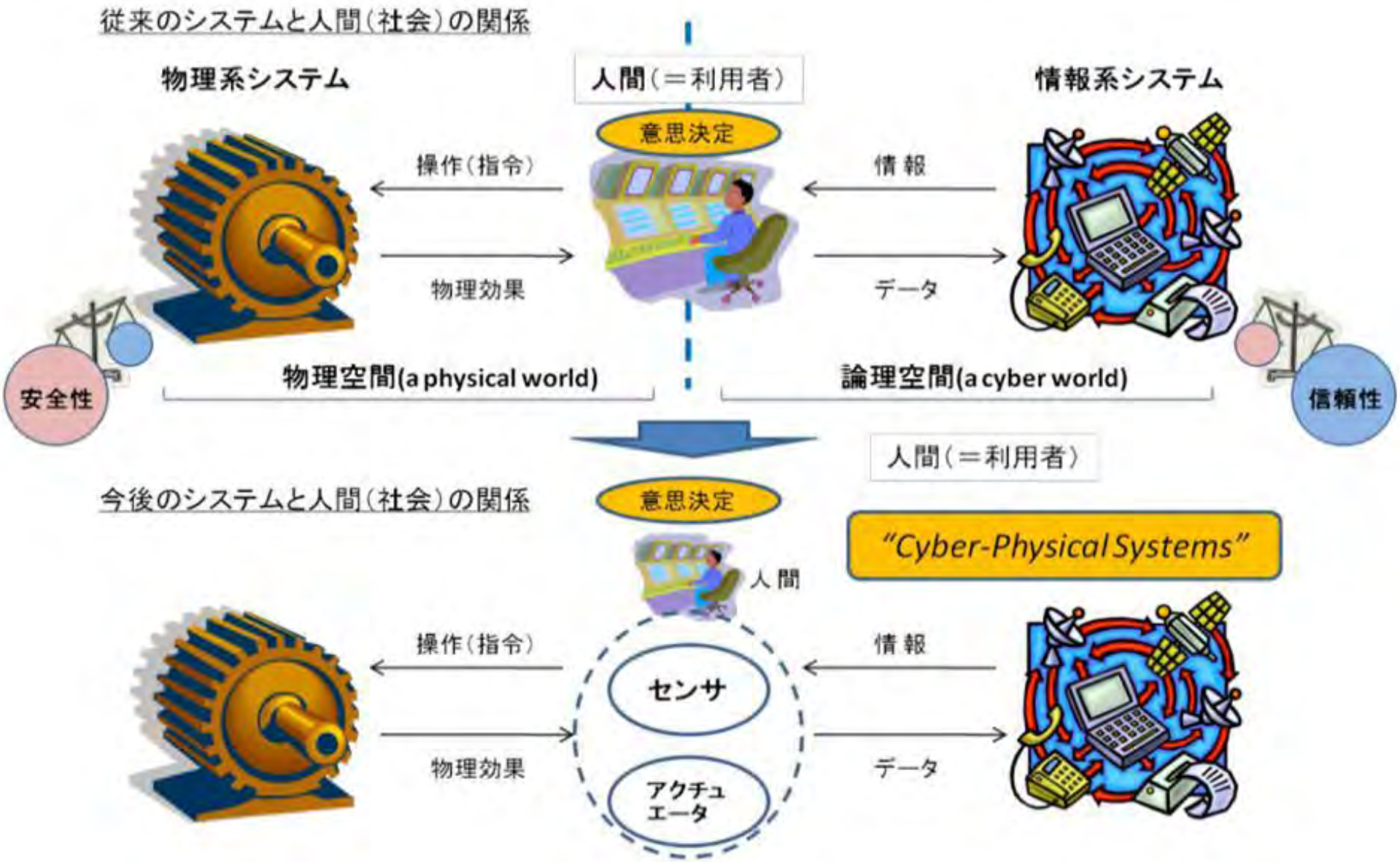
- 至る所に障害の原因は潜んでいることが推測される。
- 重篤度の高い障害は、航空管制・鉄道運航管理系のシステム。

注）番号は「重要インフラ」別の整理番号、「重大」事例については経済的損失額、障害復旧時間各々の大きい順に羅列、（）内は被害

原　因　（推定含む）

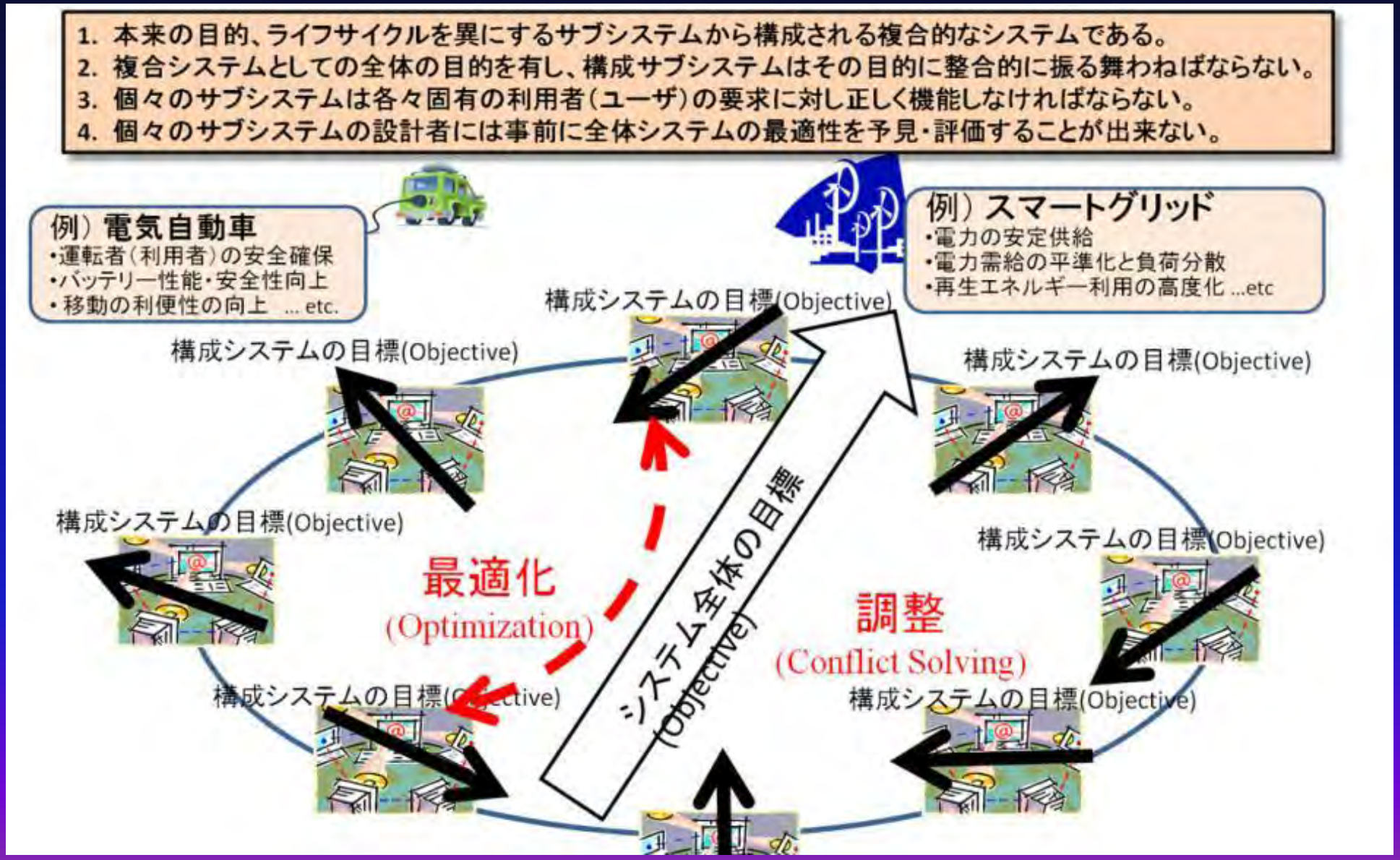
重篤度	元々の仕様・設計・構築に不具合（仕様要求不足・考慮漏れ含む）	運用・保守時に発生（アップグレード・リプレース時）	人為的なミスにより発生（管理ミス、運用ミス等）
破局的（死傷者発生・その潜在性大）	17. Boeingグアム墜落事故（死者228名） 22. 英Paddington列車衝突事故（死者31名） 32. 英Buncefield油槽所火災（警報不良）	19. 米航空管制システム障害（管制官200名） 24. 独鉄道レール切替シス不具合（3日間） 23. 米道路交通信号機シス不具合（復旧半日）	24. 米NY地下鉄衝突事故（仕様見直し不足）
重大（経済的損失大、広範囲・長期障害）	18. 英航空管制SWバグ（開発費6.2億ポンド） 10. NASDAQシステム誤作動（復旧24時間） 7. 米長距離電話通信網ダウン（復旧9時間） 8. 英LSE株式売買システムダウン（復旧7時間） 25. 欧州停電（復旧最大4時間、最大6000万人） 30. 米社会保険金支払不足（約70万人） 31. 加医療情報シス不具合（約600人、復旧5日） 1. Verizon社料金過剰請求（復旧4日） 3. スウェーデン電話不通（復旧最大8時間）	15. 北米銀行口座残高増加（7.6億ドル誤謬） 16. 米NYSE取引停止（復旧75分） 14. 北投資家口座残高不足（復旧24時間） 10. 北米銀取引シス不具合（1億ドル、復旧2週間） 4. 加Northern電話交換シス不具合（復旧1カ月） 2. 米MCI-WorldCom NW障害（復旧8日間） 20. 米列車発券シス不具合（復旧最大3日間） 6. 米AOL NWダウン（復旧19時間） 5. 米Bell Atlantic電話シス不具合（復旧7時間） 9. 米地銀システムダウン（ATM停止等）	26. 北東アメリカ大停電（人為的他複合原因） 21. 米シスコ高速鉄道停止（復旧最大70分）
その他（上記以外）	12. 米銀ATM停止（復旧最大1日） 27. 米大統領選投票シス障害（復旧最大半日）	28. 英納税システム不具合（約13万人） 29. 米財務省社会保険シス不具合（約5万人）	13. ドイツ銀傘下銀行口座誤処理（復旧2日）

問題を複雑にしている原因1（Cyber-Physical）



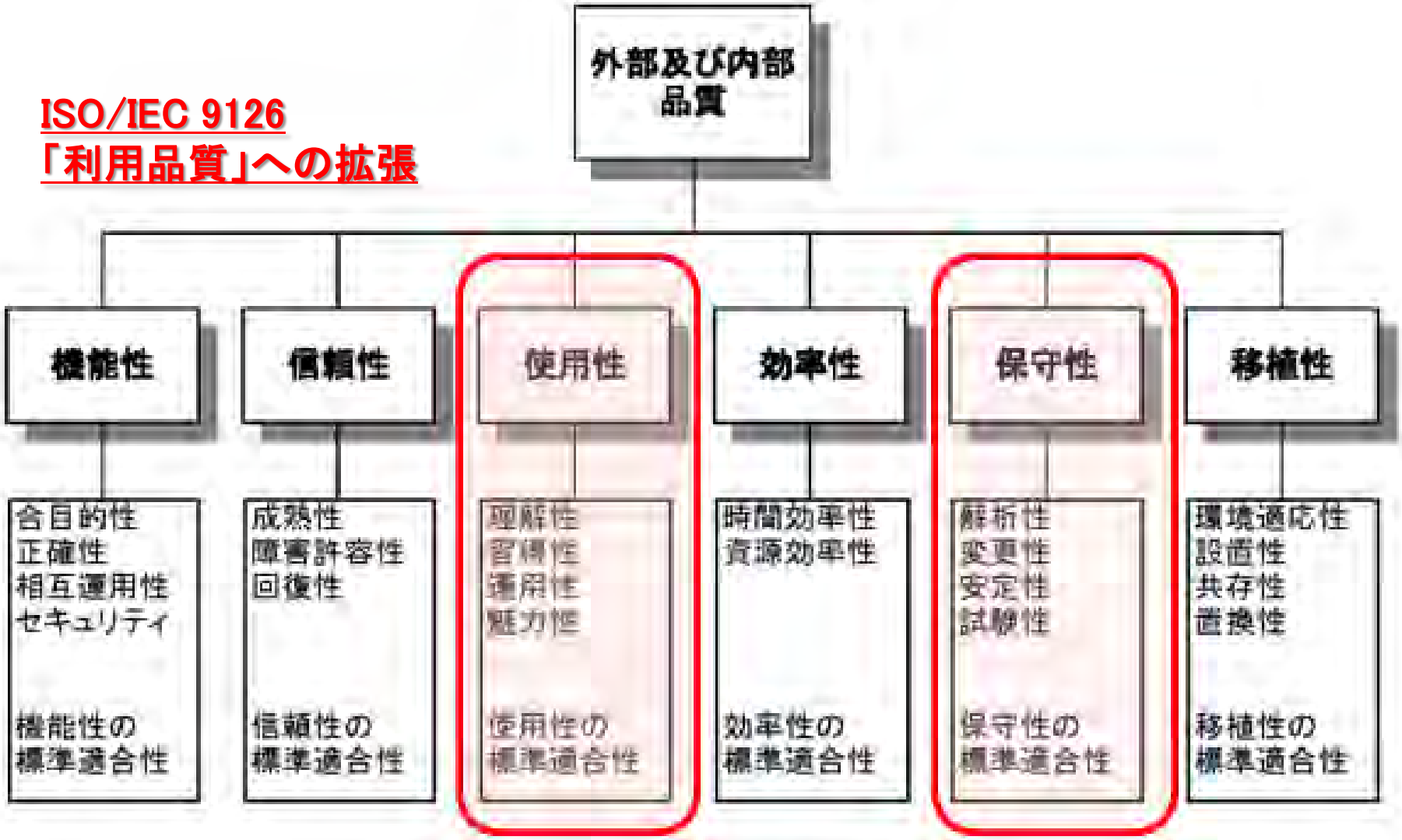
問題を複雑にしている原因2（System of Systems）

1. 本来の目的、ライフサイクルを異にするサブシステムから構成される複合的なシステムである。
2. 複合システムとしての全体の目的を有し、構成サブシステムはその目的に整合的に振る舞わねばならない。
3. 個々のサブシステムは各々固有の利用者（ユーザ）の要求に対し正しく機能しなければならない。
4. 個々のサブシステムの設計者には事前に全体システムの最適性を予見・評価することが出来ない。



問題を複雑にしている原因3（常に変化する利用状況）

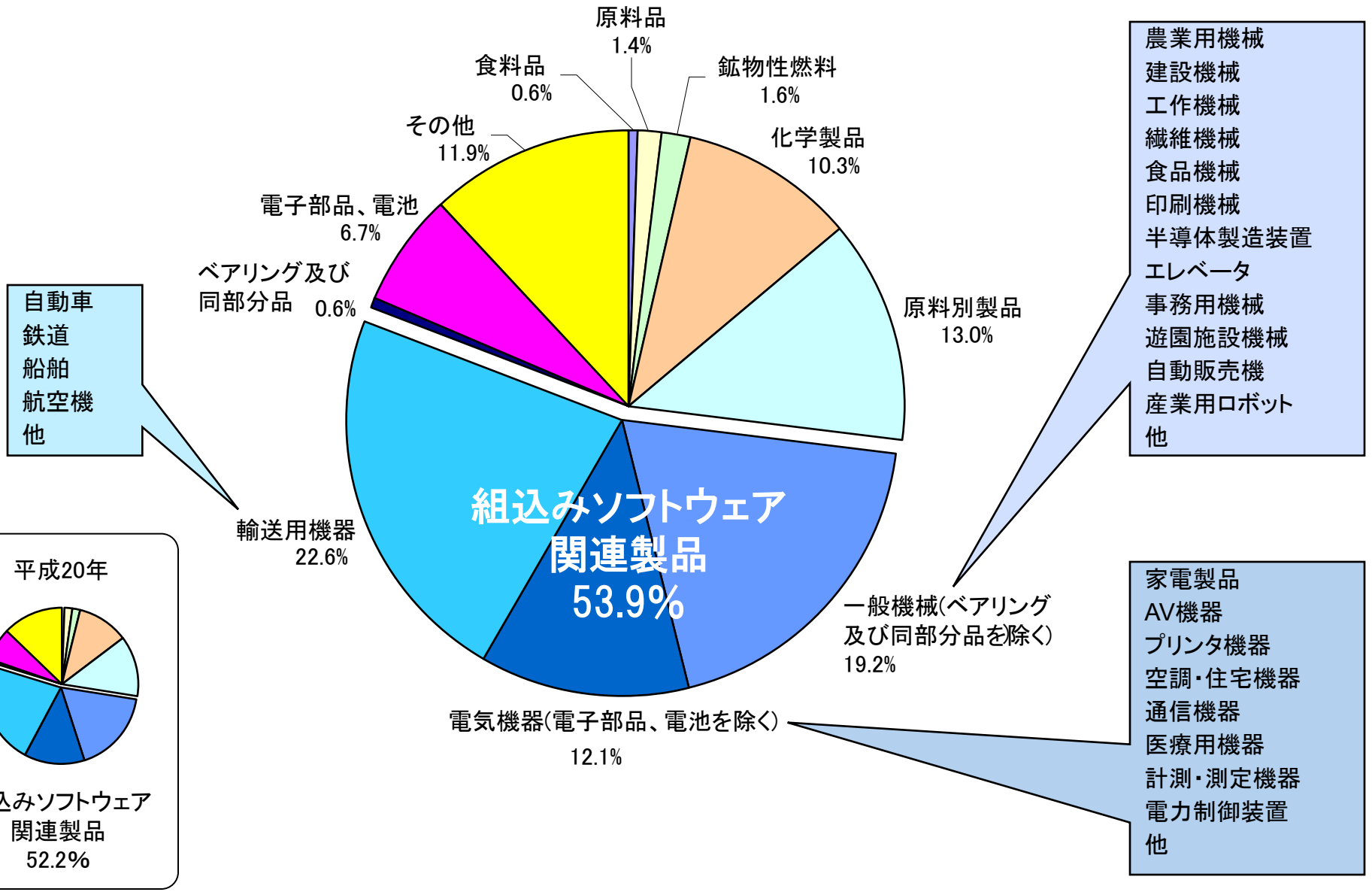
ISO/IEC 9126
「利用品質」への拡張



（出典）JIS X 0129:2003（ISO/IEC 9126:2001）

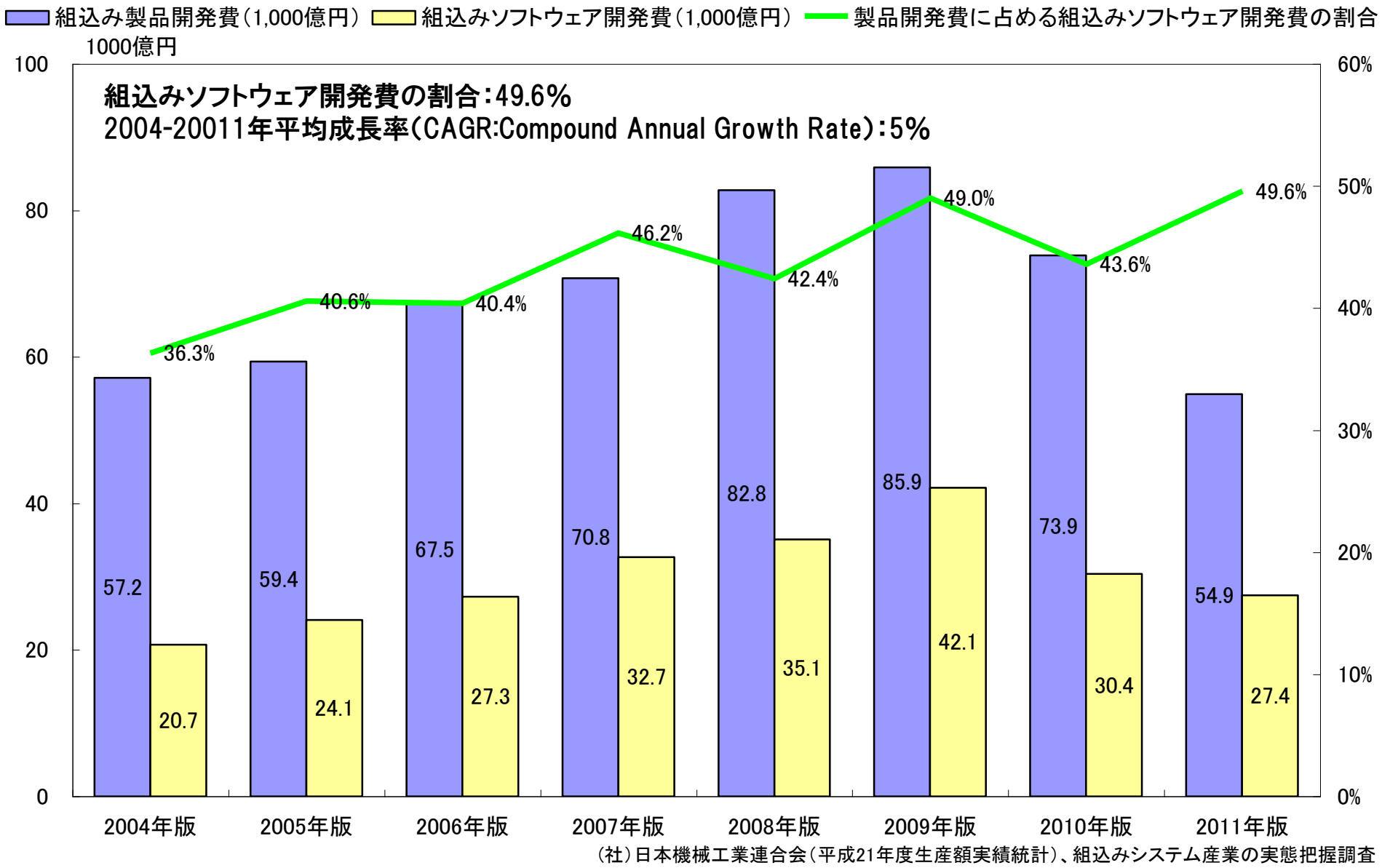
3. 日本の組込みソフトウェア開発現場の現状

平成21年のわが国の輸出に占める組込みソフトウェア関連製品



Copyright © 2011 IPA, All Rights Reserved

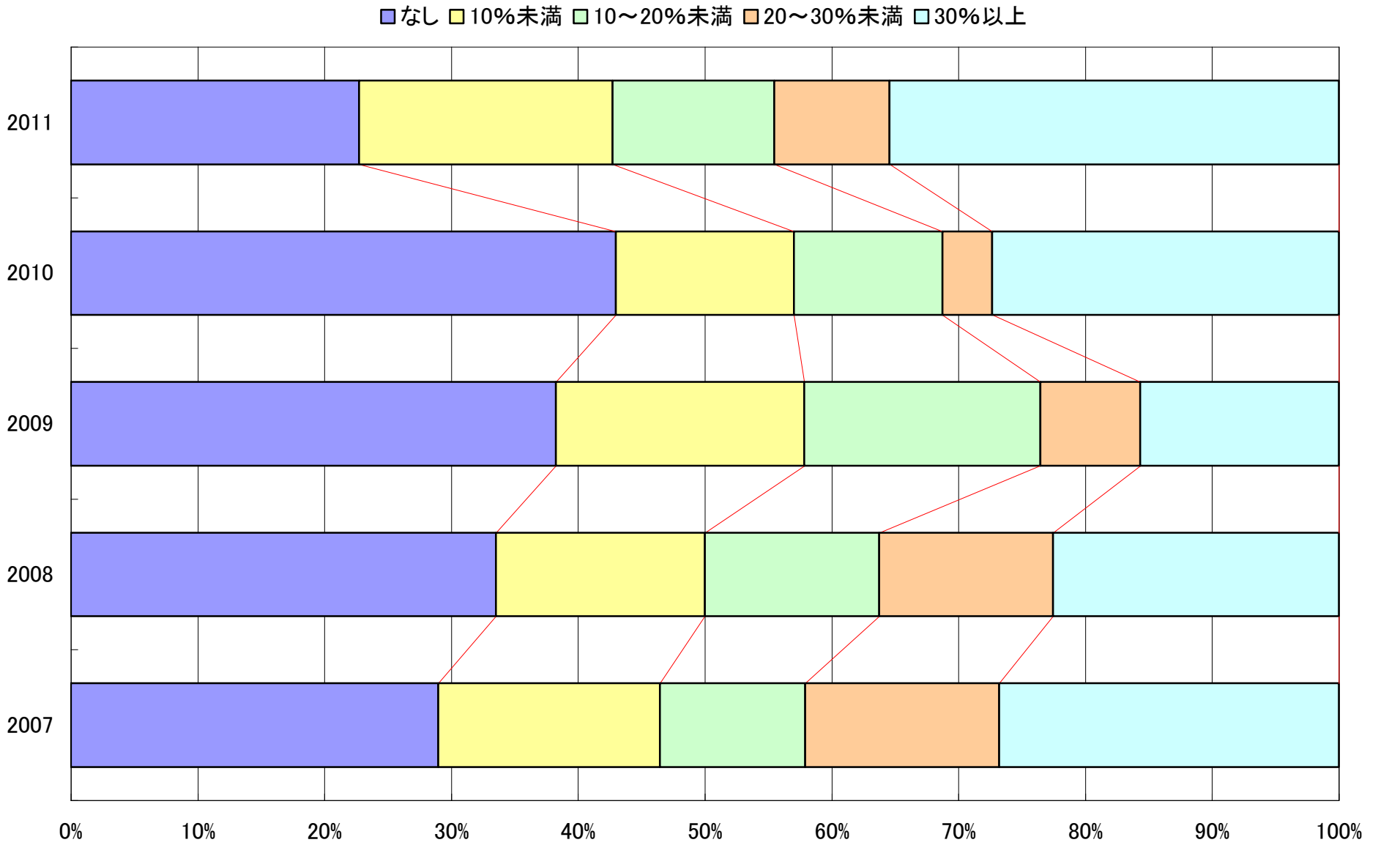
組込みシステム製品開発費と組込みソフトウェア開発費・開発費比率の推移



（社）日本機械工業連合会（平成21年度生産額実績統計）、組込みシステム産業の実態把握調査

Copyright © 2011 IPA, All Rights Reserved

製品出荷後の不具合発生製品率の推移



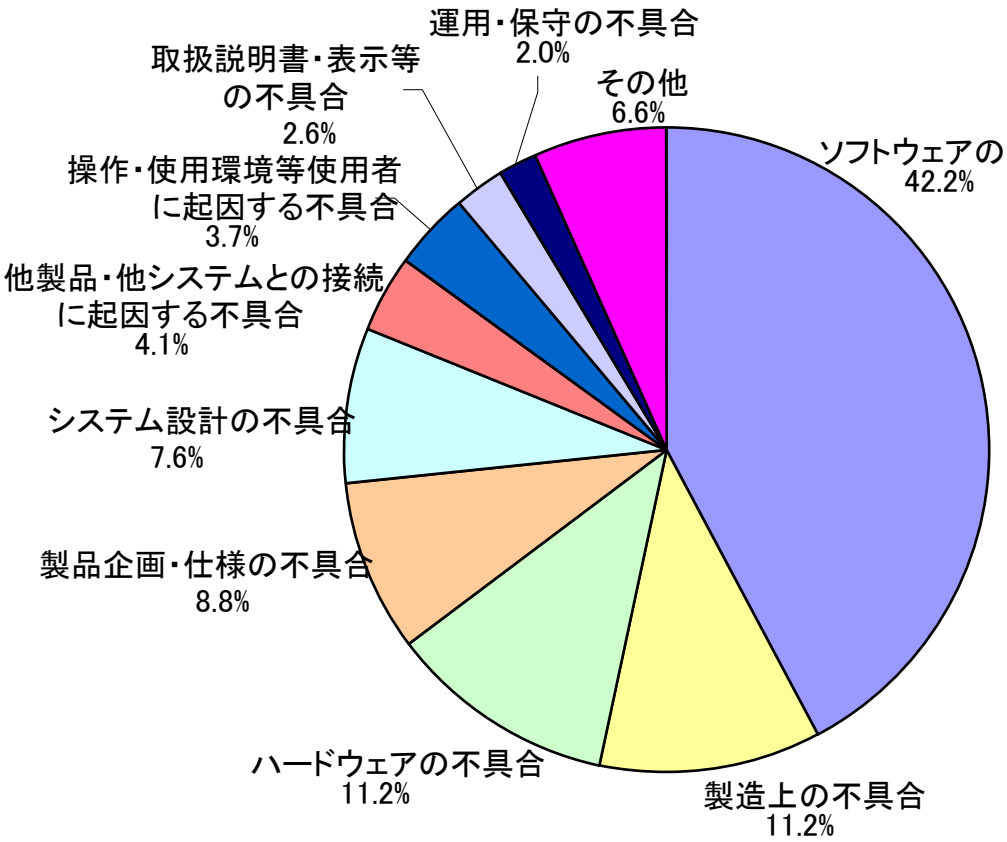
出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

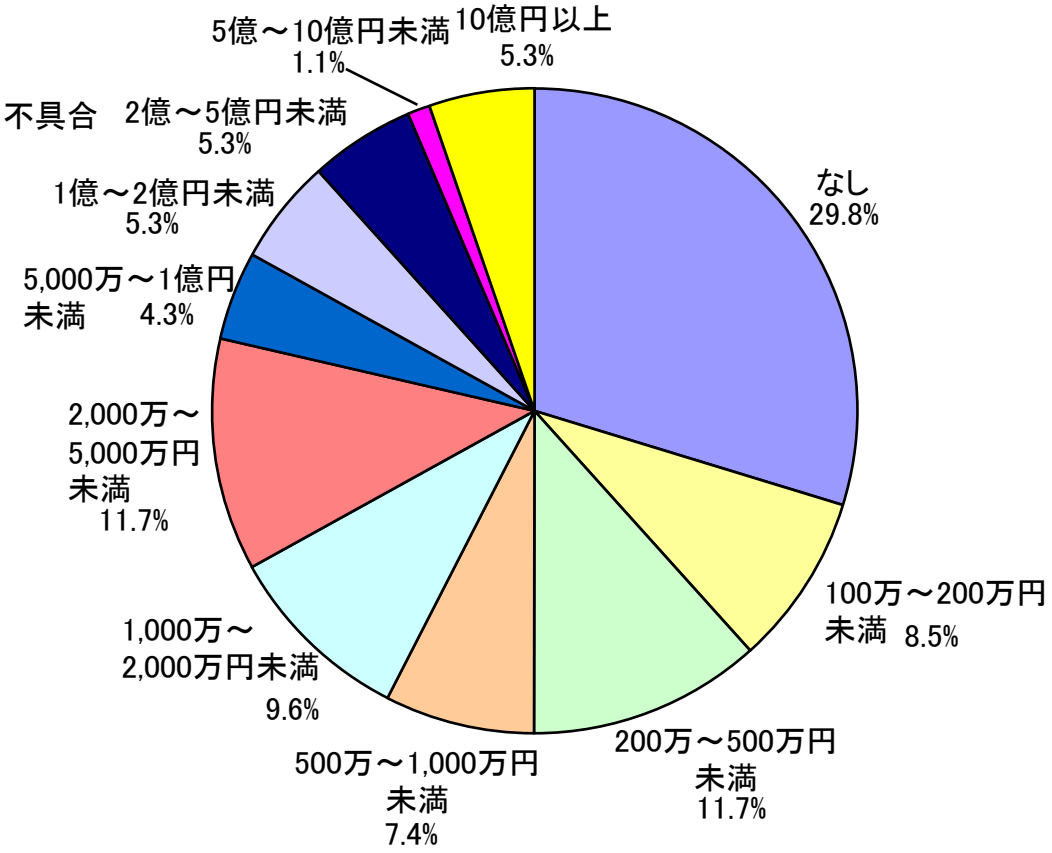
製品出荷後の不具合の原因と「対策費＋損失」

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

不具合の原因（製品数ベース）



「対策費＋損失」



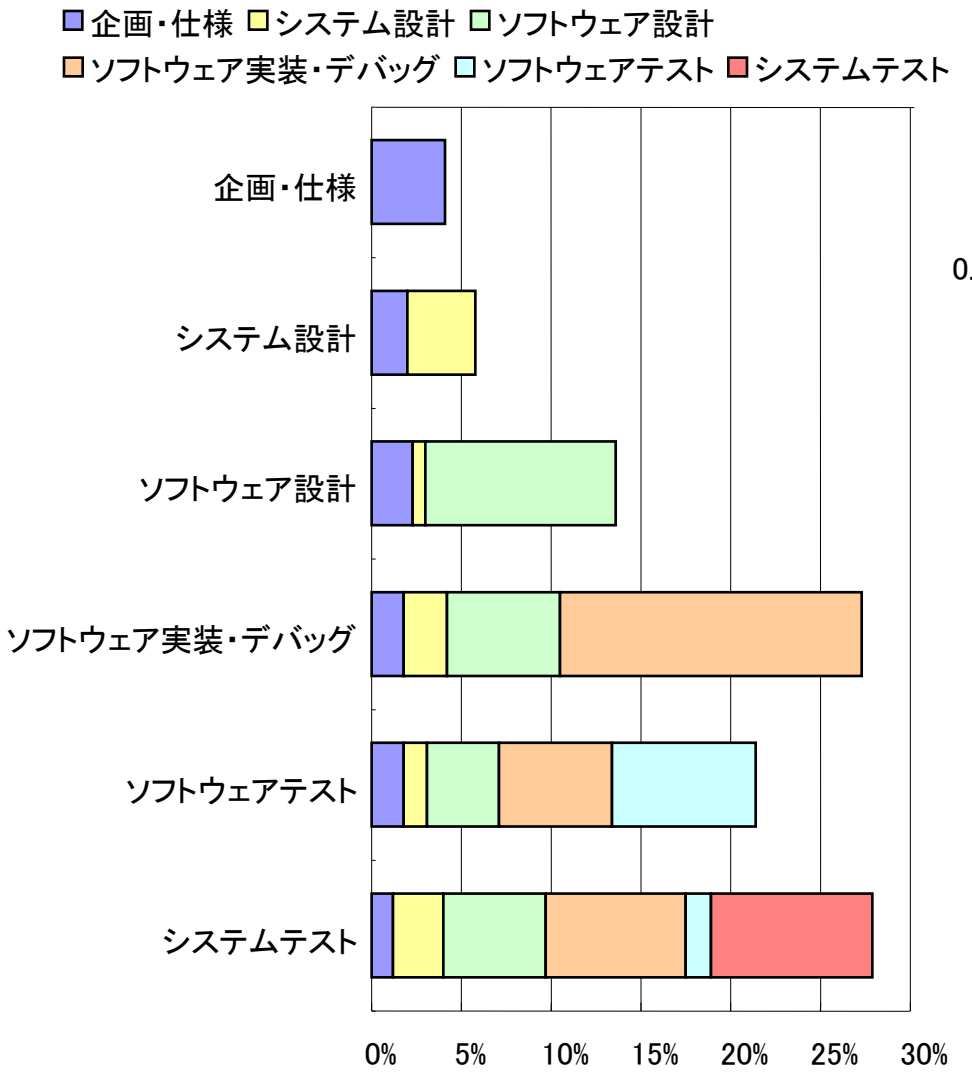
出典：「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

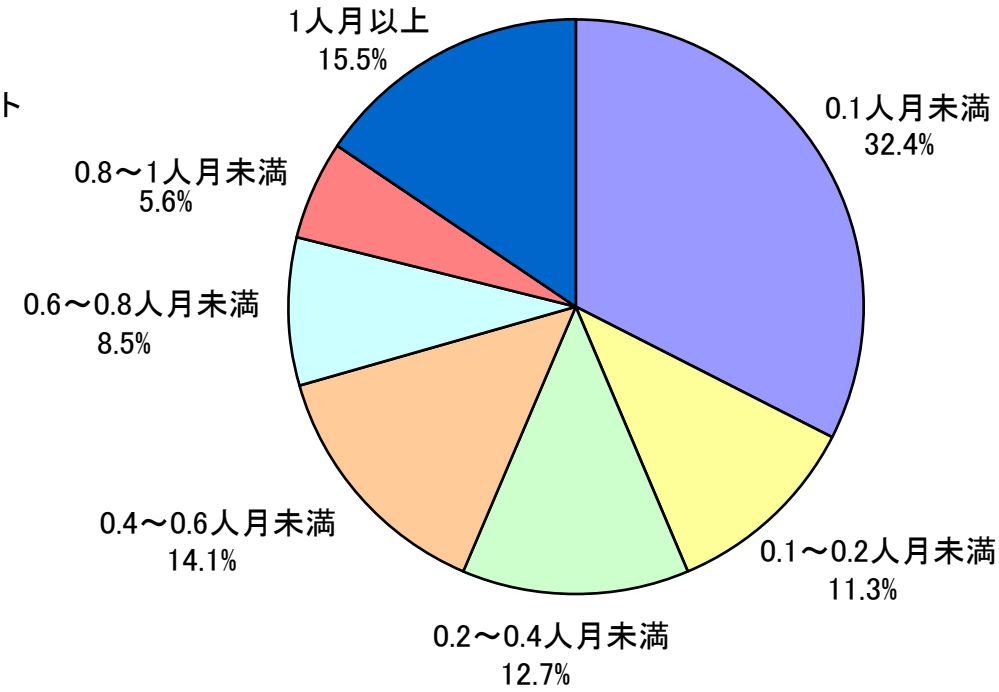
工程別不具合発見件数比率と不具合1件あたりの修正工数

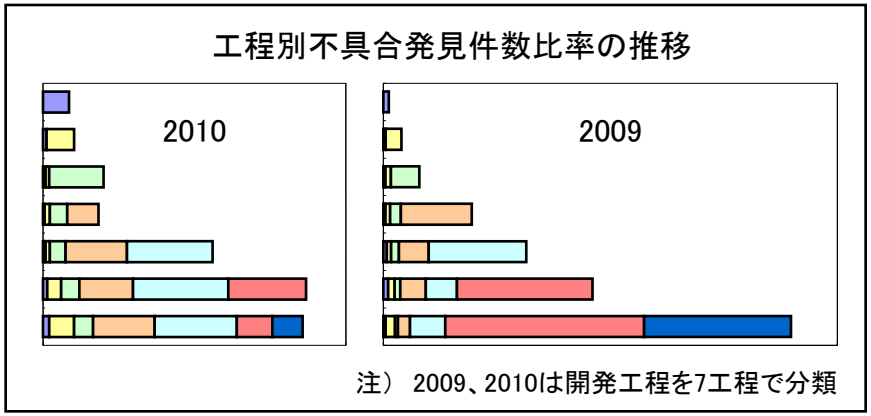
SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

工程別不具合発見件数比率



不具合1件あたりの修正工数





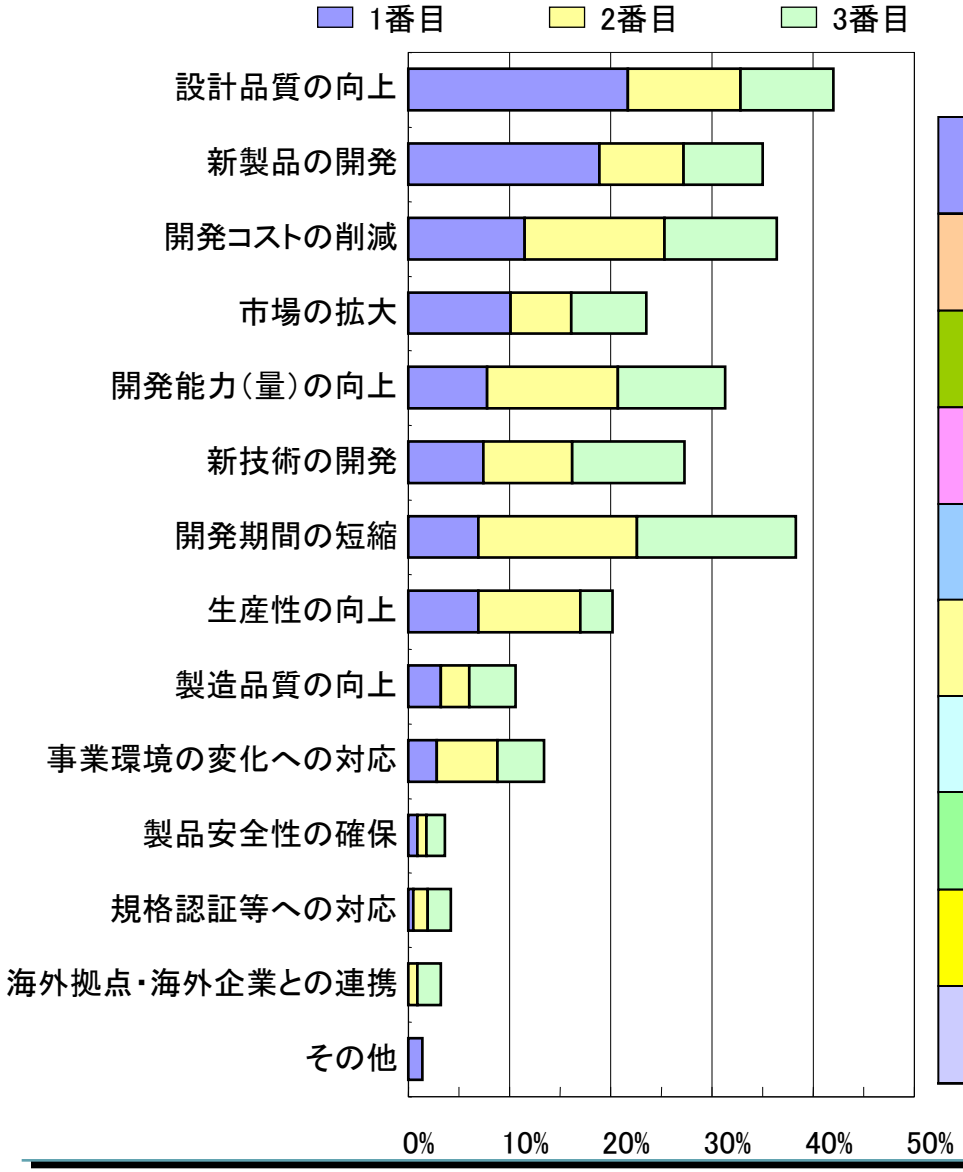
出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

組込みソフトウェア開発の課題

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

2011年組込みソフトウェア開発の課題



1番目の課題Top10の推移（2007～2011）

2007	2008	2009	2010	2011
設計品質	設計品質	設計品質	設計品質	設計品質
新製品	新製品	開発期間	開発コスト	新製品
開発期間	開発期間	生産性	新技術	開発コスト
開発能力	開発能力	開発コスト	新製品	市場拡大
生産性	開発コスト	開発能力	市場拡大	開発能力
開発コスト	生産性	新技術	開発能力	新技術
市場拡大	市場拡大	製造品質	開発期間	開発期間
新技術	新技術	新製品	製品安全	生産性
製品安全	製品安全	市場拡大	生産性	製造品質
製造品質	製造品質	製品安全	製造品質	事業環境変化対応

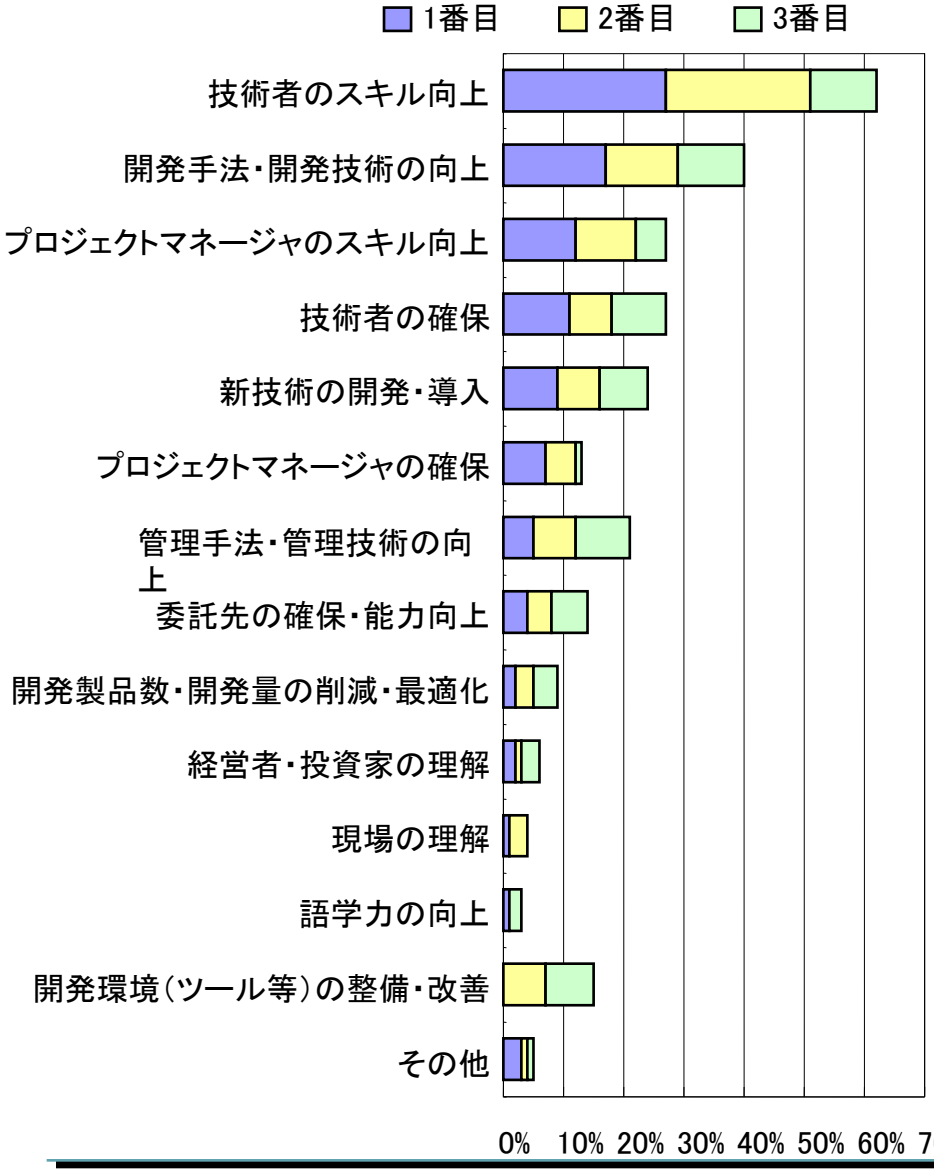
出典：「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

組込みソフトウェア開発課題に有効な解決手段

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

2011年:課題に有効な解決手段の合計



1番目の解決手段Top10の推移（2007～2011）

2007	2008	2009	2010	2011
技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上
技術者の確保	技術者の確保	PMのスキル向上	PMのスキル向上	開発技術の向上
PMのスキル向上	PMのスキル向上	開発技術の向上	開発技術の向上	PMのスキル向上
開発技術の向上	開発技術の向上	PMの確保	技術者の確保	技術者の確保
PMの確保	PMの確保	技術者の確保	新技術開発・導入	新技術開発・導入
管理技術の向上	管理技術の向上	管理技術の向上	PMの確保	PMの確保
新技術開発・導入	新技術開発・導入	新技術開発・導入	管理技術の向上	管理技術の向上
開発環境の整備	開発環境の整備	開発製品数最適化	委託先の確保	委託先の確保
開発製品数最適化	委託先の確保	開発環境の整備	開発環境の整備	開発製品数最適化
経営者の理解	経営者の理解	委託先の確保	経営者の理解	経営者の理解

出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

組込みソフトウェア開発課題に有効な解決手段(課題別)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

課題＼有効な解決手段	技術者のスキル向上	開発手法・開発技術の向上	プロジェクトマネージャのスキル向上	新技術の開発・導入	技術者の確保	開発環境(ツール等)の整備・改善	管理手法・管理技術の向上	委託先の確保・能力向上	プロジェクトマネージャの確保	開発製品数・開発量の削減・最適化	経営者・投資家の理解	現場の理解	語学力の向上	その他
設計品質の向上	68	44	31	15	27	19	27	10	14	10	6	5	2	1
新製品の開発	45	20	31	53	24	7	8	13	13	4	8	5	4	8
開発コストの削減	53	53	41	9	7	25	32	21	7	18	3	4	1	0
市場の拡大	28	9	17	39	20	4	11	20	17	9	15	9	7	20
開発能力(量)の向上	68	44	24	13	43	21	12	15	7	4	3	4	6	1
新技術の開発	66	30	14	70	38	5	0	9	7	5	7	4	4	2
開発期間の短縮	57	46	28	9	29	34	35	15	5	14	0	1	3	0
生産性の向上	73	55	32	11	9	43	25	9	5	5	2	7	0	2
製造品質の向上	73	36	32	36	32	0	32	14	18	23	9	14	0	5
事業環境の変化への対応	34	14	24	45	14	7	7	17	3	7	38	21	14	10
製品安全性の確保手段	88	13	25	13	25	25	38	0	0	13	0	0	0	0
規格認証等への対応手段	38	0	25	0	13	38	50	50	0	0	25	0	25	0
海外拠点・海外企業との連携手段	17	0	33	17	17	0	0	33	0	0	0	33	100	17
全体の平均	58	39	28	26	25	20	20	14	9	9	5	5	3	4

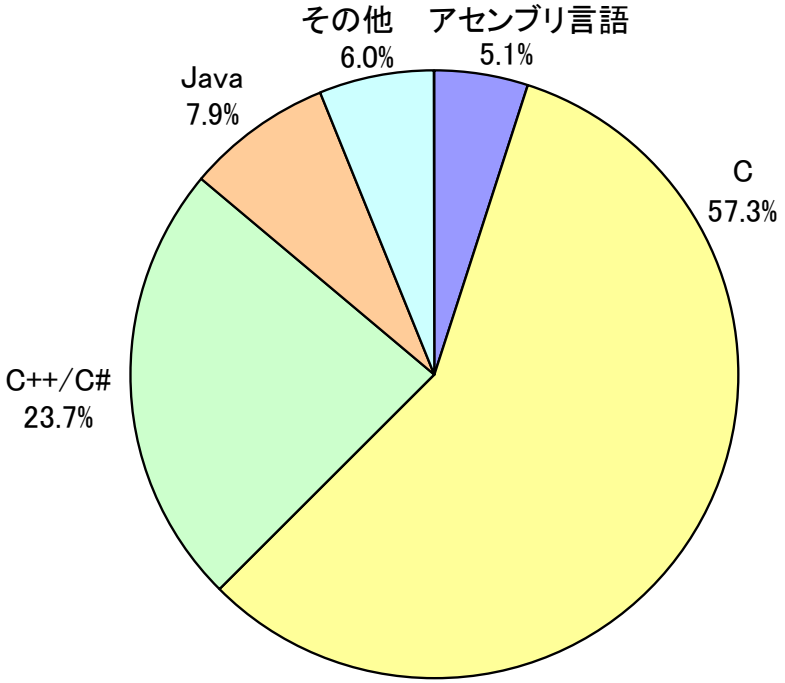
注:枠内の数字は課題に有効な解決手段として挙げられた1番目から3番目の合計の%

出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

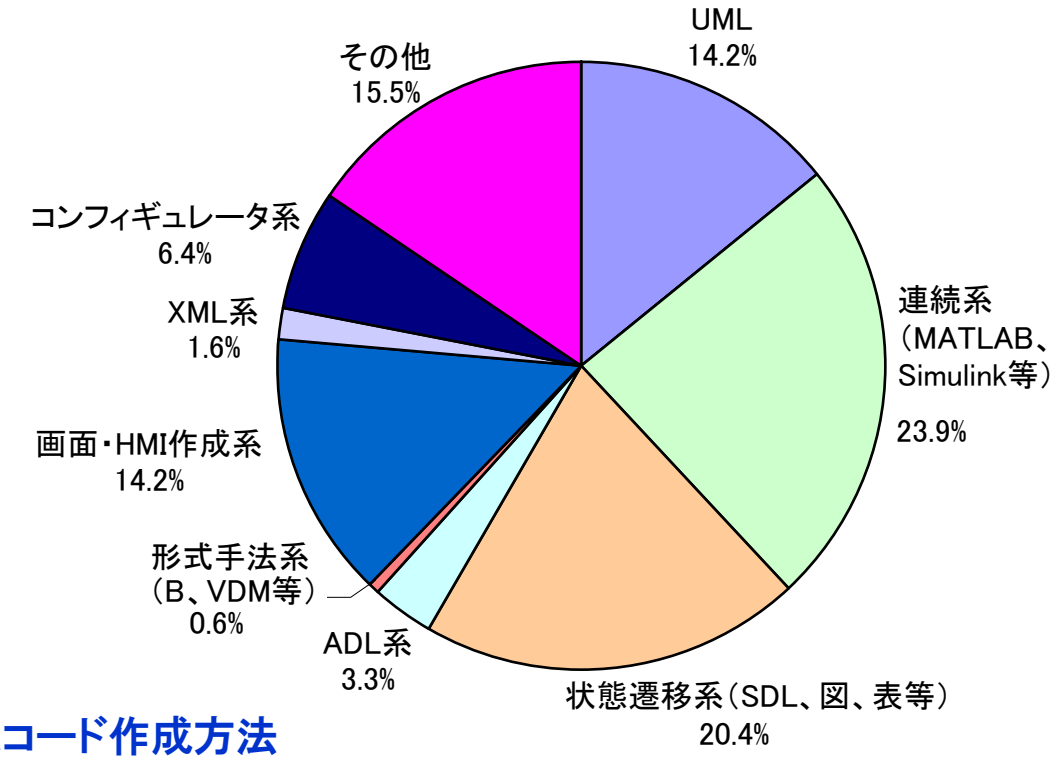
Copyright © 2011 IPA, All Rights Reserved

使用しているプログラミング言語

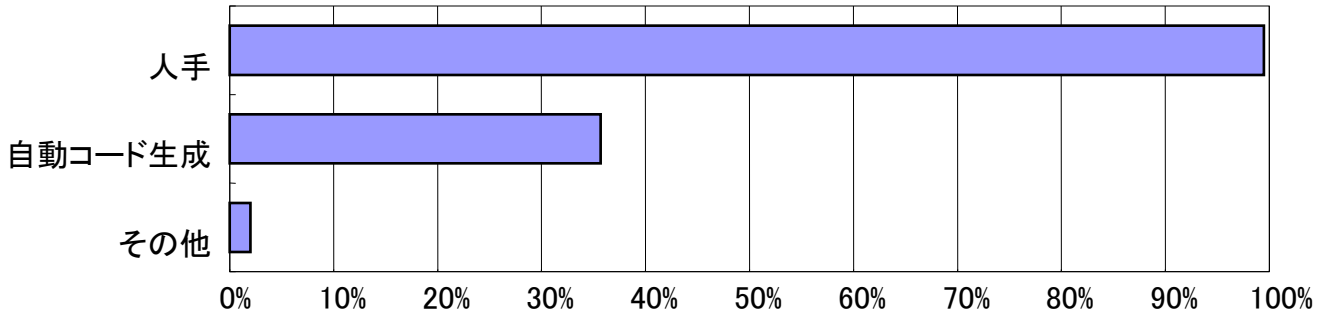
使用しているプログラミング言語(人手)



使用しているモデルベース言語(自動コード生成)



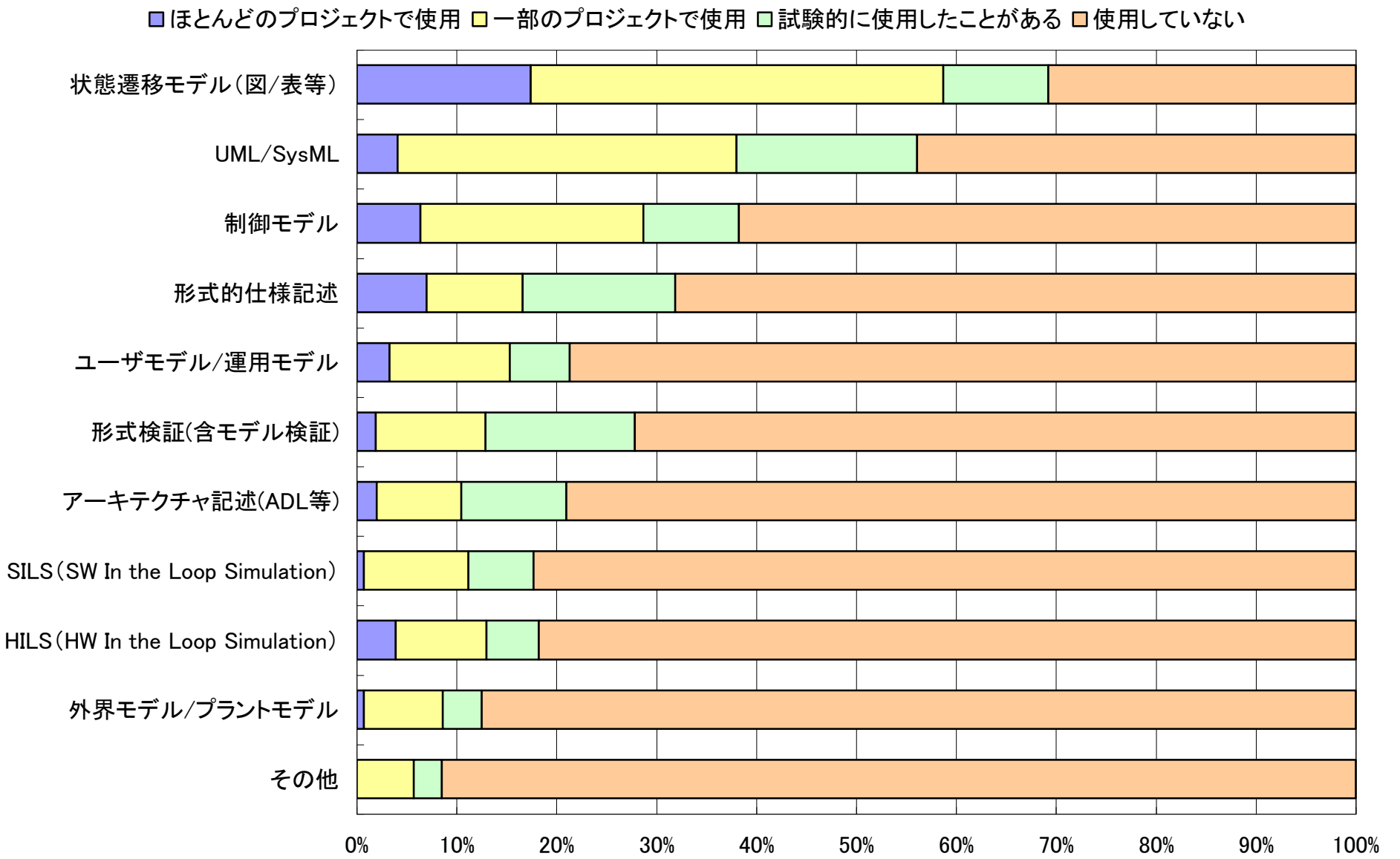
プログラムコード作成方法



出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

モデルベース開発技術の利用状況



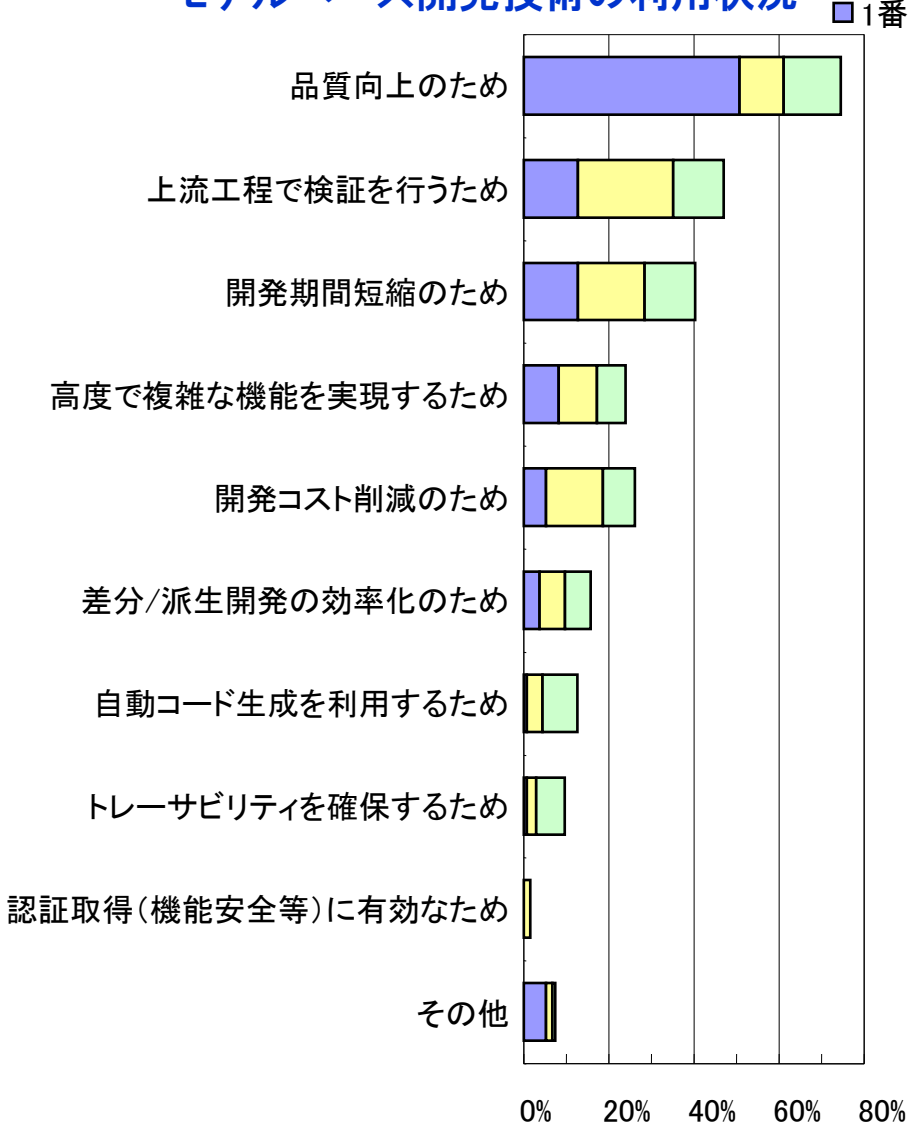
出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

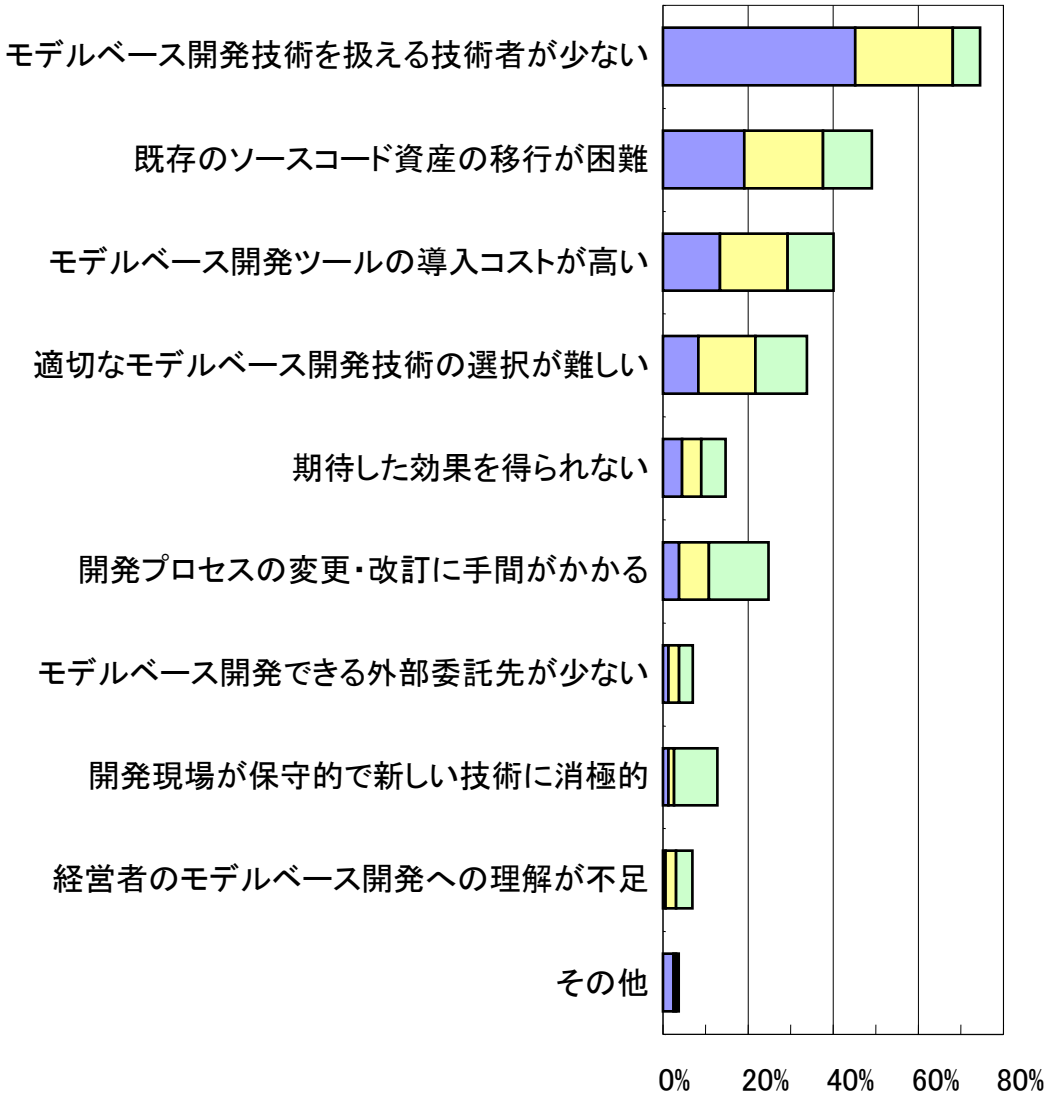
モデルベース開発技術を利用した理由と課題

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

モデルベース開発技術の利用状況



モデルベース開発技術利用の課題



出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

組込みソフトウェア開発を取巻く事業環境の変化(1)

- 機能安全、第三者検証・妥当性確認など品質説明力の向上
  - 機能安全規格と第三者検証・妥当性確認の両者に対応した組込みソフトウェア開発(組込みソフトウェア開発に関わる全ステークホルダの対応が必要)
  - 対応した開発情報管理
    - 開発情報のトレーサビリティーの確保
    - 開発に関わる技術活動記録、組織活動記録などのエビデンス収集
  - 開発に使用する開発ツールの認証取得
  - 説明力(証明力)の高い開発技術の適用
    - 形式手法、モデルベース手法など
- 実装中心から設計中心のソフトウェア開発への移行
  - 実装工程の海外アウトソースと機械化(自動コード生成ツール)の拡大により国内の開発は上流工程中心に移行
  - 上流工程の中核技術はモデルベース(モデル駆動)開発技術
    - 開発プロセスのモデルベース開発への適応(上流工程での設計検証など)
    - 開発ツール等の導入(モデルベース開発技術はツール支援を前提とした開発技術)
    - モデルベース開発技術を扱える上流工程技術者の育成
      - 基礎的な学力(数学、論理学など)が不足しているソフトウェア技術者の育成
  - 利用者情報、利用情報の活用
    - 要求獲得、要件定義、・・・

Copyright © 2011 IPA, All Rights Reserved

組込みソフトウェア開発を取巻く事業環境の変化(2)

- 組込みシステムの他システムとの統合化(統合システム化)
  - 自動車の例:車載システムの統合化と並行して、車外システムとの統合化が進行
    - 電動機の採用による、スマートエネルギーシステムと統合化
    - インターネット等との接続による、情報システムと統合化
    - ITSなどの高度交通システムへの対応による、交通インフラや他の車両と統合化
    - 他産業との連携したシステム開発
      - 住宅産業、電力産業、家電産業、情報サービス産業など
  - 全体システムとしての安全性・信頼性の確保
    - 共通モデルによる上流段階での検証　など
- 開発拠点のグローバル化
  - リーマンショック後の円高に対応するため開発拠点の海外展開が進行
    - プラザ合意以降の円高に対応して生産拠点については海外展開が進行した(自動車産業では約4割が海外生産)
    - 2008年度までの国内組込みソフトウェア技術者の不足(約10万人不足と言われた)に対応するため海外拠点での技術者確保、海外へのアウトソーシングが拡大した
    - 既に海外拠点が存在し、海外でのソフトウェア開発経験も積んでおり、開発拠点の海外展開を進める土壌はできている
    - 今後、国内の開発リソース需要は減少(特に、ソフトウェア実装・テストの外部委託は、海外移転と自動化などにより国内市場は消滅)
  - 国内組込みソフトウェア産業の構造改革が急務

Copyright © 2011 IPA, All Rights Reserved

4. SECにおける統合システム信頼性向上への取組み

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

監査対象

- ソフトウェア・プロダクト
- 開発プロセス

評価

監査機関
監査人

- 資格
- スキル／能力

監査基準

- 基準となる品質特性
- 基準となる手法
- 基準となるプロセス など

- 共通／分野別
- 公平性／専門性／最新性
- 国際性

基準を支える知見

- 高品質ソフトウェア開発・管理技術
  （要件定義・上流設計・テスト
  プロセス改善・定量的管理など）

品質問題の多くは要件のエラー
しかも、
人間（利用者、運用者）に絡む
↓
上流・超上流に重点

高信頼システム開発技法としての形式手法

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

形式手法の適用

- 要求定義段階での曖昧性・矛盾の排除と欠陥の早期除去
- 要求～設計～実装～テストまでのトレーサビリティの確保
- 形式検証によるテストの自動化
- 関係者全ての間での知識共有とコミュニケーションの円滑化

SECにおける統合システム信頼性向上への取組み

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

監査対象

- ソフトウェア・プロダクト
- 開発プロセス

評価

監査機関
監査人

- 資格
- スキル／能力

監査基準

- 基準となる品質特性
- 基準となる手法
- 基準となるプロセス など

- 共通／分野別
- 公平性／専門性／最新性
- 国際性

基準を支える知見

- 高品質ソフトウェア開発・管理技術
  （要件定義・上流設計・テスト
  プロセス改善・定量的管理など）

品質問題の多くは要件のエラー
しかも、
人間（利用者、運用者）に絡む
↓
上流・超上流に重点

ソフトウェア品質監査制度(仮称)検討の背景と経緯
第三者の検証・妥当性確認による品質説明力強化の必要性

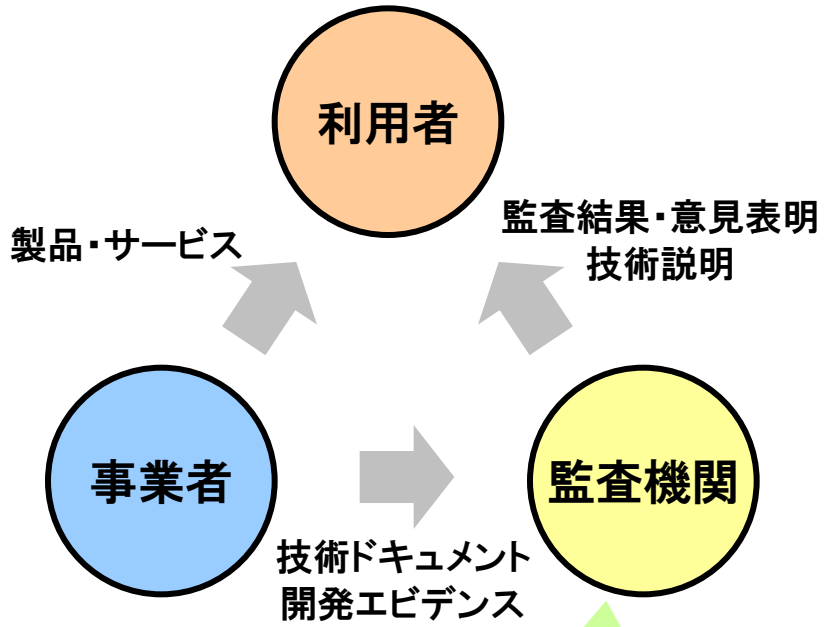
SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

品質説明に対する市場意識の変化
品質説明力の不足： 当事者企業の技術的主張だけでなく、第三者の裏付け(検証、妥当性確認)による品質説明への要求の増大

製品の利用者が感じる違和感
利用品質低下の懸念： 製品・システムの高度化・複雑化と利用者の多様化により、製品・システムと利用者との間のギャップが拡大

先端技術製品の潜在リスクへの不安
製品品質低下の懸念： 技術の急速な進歩により技術標準(規格)に基づく規格認証の対象範囲外となる領域が拡大

品質文化の異なる業界を跨るシステム
残存する潜在リスクの増加： 複数の業界を跨るシステムの拡大に伴い、全体システムとしての品質確認の精度が低下



第三者による検証・妥当性確認
事業者の技術的主張の妥当性を、監査機関が開発技術水準と利用技術水準を考慮して第三者の立場で評価し、技術に関する専門知識のない利用者にも理解できる形で情報提供する仕組み

(会計処理における会計監査と同等の役割)

IPA/SECでの活動経緯
- 2010年3月：産構審情報システム・ソフトウェア小委員会にて第三者による検証・妥当性確認の枠組みの必要性が示される
- 2010年4月：IPA/SECの統合系プロジェクト内に検討チームを発足
- 2010年7月：調査活動開始
- 2010年11月：制度検討委員会発足(主査：名古屋大学高田教授)
- 2011年4月：中間報告(予定)

Copyright © 2011 IPA, All Rights Reserved

ソフトウェア品質監査制度(仮称)の狙いと効果

国民生活の安全・安心・快適の向上と我が国産業の国際競争力の強化

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

ソフトウェア品質監査制度(仮称)の狙い	ソフトウェア品質監査制度(仮称)の効果
企業の製品・システムに関する利用者や市場への品質説明力の強化	技術の専門家ではない利用者の安心感の向上
国際市場における日本製品・システムの品質に対する正当な評価の確立	我が国産業の国際競争力の維持・強化
産業界の枠を超えた品質の見える化による複数の産業界を跨り構成される高度なシステムの開発加速 (例:スマートコミュニティシステムなど)	国民生活の快適性・利便性の向上 新成長戦略分野における我が国産業の国際優位性の確保
製品・システムの本質的な品質向上	国民生活の安全性の確保

ご参考:米国の状況

- 2010年日本製自動車の制御システムに対する不具合の疑念が拡大。米国政府の要請で、NASAの独立検証・妥当性確認(IV&V)センターが第三者の立場で、制御システムの検証ならびに妥当性確認を実施。2011年2月、不具合が発見されなかったとの最終報告が公開。
- 当事者企業の主張だけでなく、第三者の主張がないと説明力が不充分との意識
  (会計処理における会計監査の必要性と同等の意識)。
- 国防省やNASAのシステムの調達、航空機分野、医療機器分野で類似した仕組みを運用している。

Copyright © 2011 IPA, All Rights Reserved

品質問題に起因する影響の度合いに応じて監査内容を定義
要求される品質説明力と監査コストとのバランス

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

利用者・国民への影響度と産業界・経済への影響度によりレベル分け(監査レベル)し、監査レベル毎に監査内容を定義する。

監査レベル

産業・経済影響レベル ＼ 利用者・国民影響レベル	0	1	2	3	4
4	4	4	4	4	4
3	3	3	3	3	4
2	2	2	2	3	4
1	1	1	2	3	4
0	0	1	2	3	4

監査レベルに対応した監査内容

監査レベル	監査する審査項目	監査方法	独立検証
4	全項目	網羅監査(全件監査)	必須
3	重要項目	網羅監査(全件監査)	必須
	その他の全項目	抜取監査(サンプル監査)	任意
2	全項目	抜取監査(サンプル監査)	任意
1	重要項目	抜取監査(サンプル監査)	任意
0	非対象	非対象	非対象

産業・経済影響レベル

レベル	影響の範囲
4	我が国の産業への広範囲な影響
3	当該産業に限定された影響 当該企業以外の同一・類似産業のへの影響
2	当該企業に限定された影響 当該製品・サービス以外の他事業への影響
1	当該製品・サービス事業に限定された影響
0	影響はない／ほとんど影響はない

利用者・国民影響レベル

レベル	影響の範囲・程度
4	当該利用者ならびに当該利用者以外への重大な影響(代替手段による影響軽減が困難な影響) 国民への広範囲で重大な影響
3	当該利用者への重大な影響に加え、当該利用者以外への軽微な影響(代替手段による影響軽減が容易な影響)
2	当該利用者に限定された重大な影響
1	当該利用者に限定された軽微な影響
0	影響はない／ほとんど影響はない

Copyright © 2011 IPA, All Rights Reserved

ソフトウェア品質監査制度（仮称）の枠組み

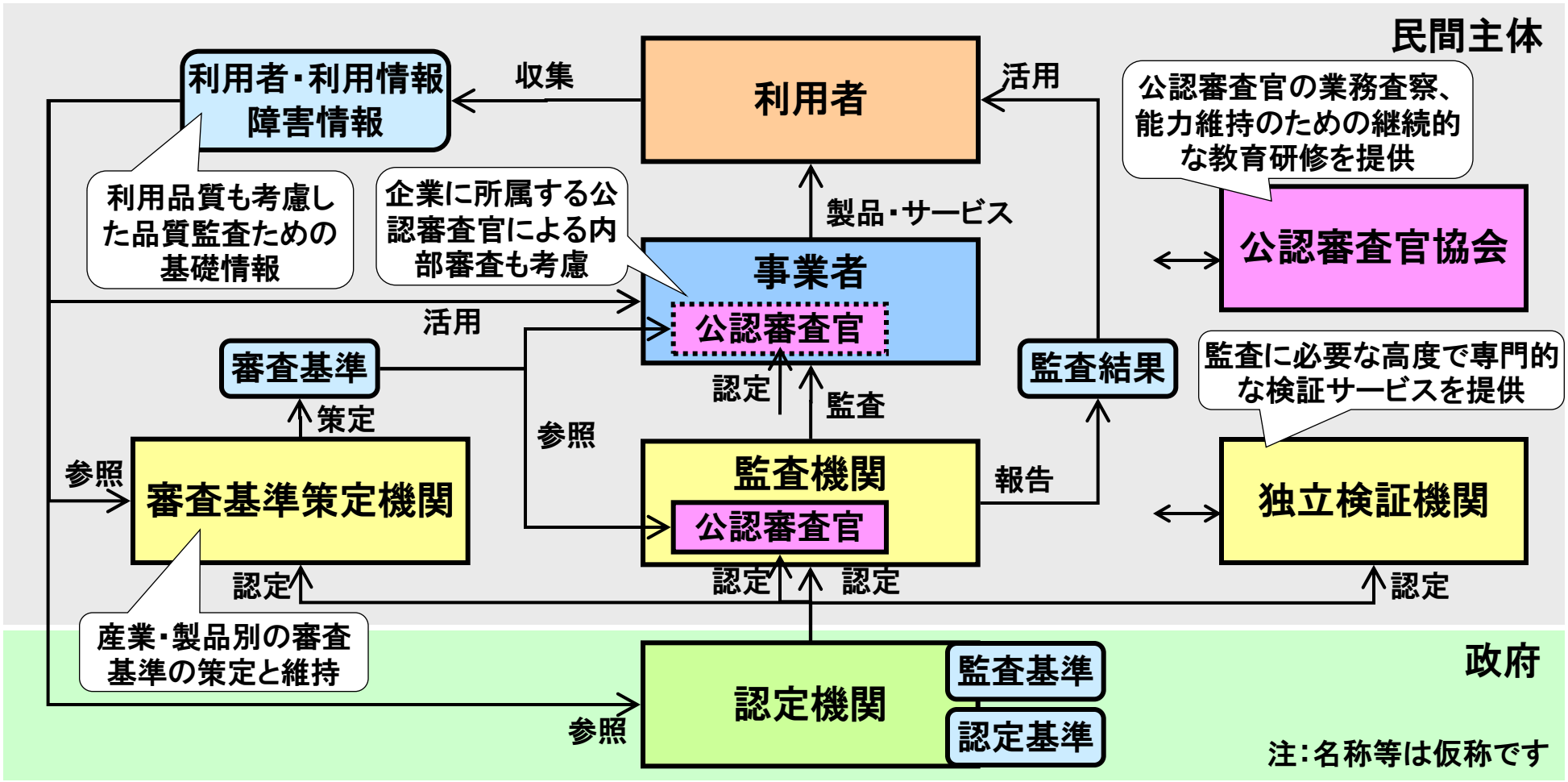
産業・製品分野別への対応と内部監査を考慮したフレームワーク

SEC
Software Engineering for Mo・No・Zu・Ku・Ri

下記の要件を満たす「公認審査官」が、産業分野あるいは製品分野毎に定められた「審査基準」を基に、「監査基準」に従って監査業務を遂行し、「監査結果」を利用者にも理解できる形で情報提供する制度

要件1. 専門性：情報の信頼性を保証できる専門知識と能力を有していること

要件2. 独立性：監査対象の事業者・利用者から身分的・経済的・精神的に独立していること



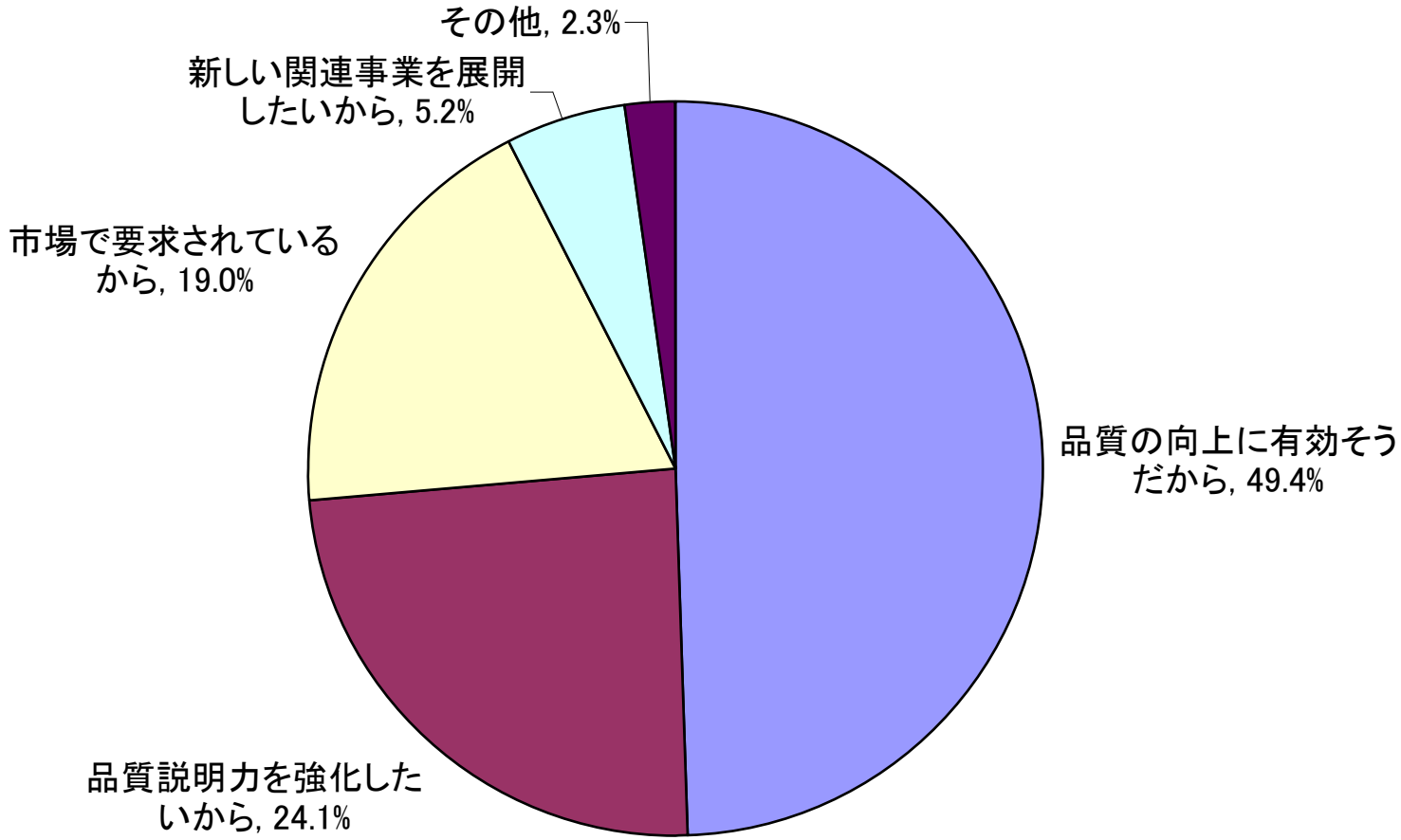
Copyright © 2011 IPA, All Rights Reserved

高信頼性システム開発を実現するための基準

- ISO/IEC15408のEAL5～7(情報セキュリティ評価標準)
- IEC61508のSIL4(電子機器の機能安全に関する国際規格)
- ISO26262(IEC61508をベースとする自動車用組込みSWの機能安全に関する規格)
- RTCA DO-178B : Software Considerations in Airborne Systems and Equipment Certification (航空用SWの開発ガイドライン)
- Safety Related Software for Railway Signaling(鉄道信号システムおよび鉄道システムに関する規格)

Copyright © 2010 IPA, All Rights Reserved

ESECの来場者へのアンケート結果(回答数:1985名)
「どのような観点で関心がありますか？」



Copyright © 2011 IPA, All Rights Reserved